SODA

MIT Connection Science
the technology of innovation

Interoperability Standards for Digital Assets

Why we need them

How to create them

How to join us

ADIA Lab
appliedblockchain
ARCHAX
Canton
Chainlink
ENTERPRISE ETHEREUM ALLIANCE
ERC3643 Association
Fireblocks
GFT
udpn
GLEIF Enabling global identity Protecting digital trust
ICMA
Interledger FOUNDATION
KEY STATE CAPITAL
LF DECENTRALIZED TRUST
LayerZero.
Libeara
Matter Labs
r3.
SOLANA FOUNDATION
Stellar
TOKENOVATE
APEX
tokeny
TRAVERS SMITH
Veridian by Cardano Foundation
WORMHOLE
XRP LEDGER
ZKsync

Interoperability Standards for Digital Assets

Page

Section 1

Introduction

The story so far: The Interoperability Group (IOG)

This endeavour has been many years in the making for Chris Ostrowski, Thomas Hardjono and Anthony Ralphs. Chris (SODA Services Ltd.), Thomas (MIT Connection Science) created the Interoperability Group (IOG) in 2022 in response to the threat of blockchain fragmentation in financial services with early contributor Anthony (novamodus.xyz) joining the group in 2025. Many financial institutions spent the early 2020s tokenizing regulated financial instruments for the first time. Working with token solution providers and blockchain foundations, banks and asset managers have issued and traded financial products in new, tokenized forms.

This has spawned many new specialist companies and an entirely new eco-system of interoperability solutions, which in simple terms, allow an asset (or a representation of the asset) to move from an existing database onto a blockchain, and in some cases between one blockchain and another.

The purpose of the IOG has been to bring together the technologists and the businesspeople who are tokenizing real world assets to agree on a common approach to enable seamless interoperability between existing databases and blockchains, and between one blockchain and another. The SODA-MIT Charter was created by the IOG in 2023 as a statement of intent by many blockchain foundations. Rather than seeking to set the standards, the Charter lists the functional requirements for any technology solution that wishes to host a regulated security. There must, for example, be an identity solution so the counterparties can be identified, a dispute resolution mechanism, a revocation mechanism and so on.

"The tokenized Real World Asset Market reached as estimated $24 billion in size in June 2025. This represents less than 0.01% of the $247 trillion of assets under management globally. Without interoperable standards tokenized real world assets will only deliver micro-efficiencies in global finance."
Chris Ostrowski, SODA Services Ltd.

Chris Ostrowski

Thomas Hardjono

Anthony Ralphs

January 2026

Developing interoperability standards for digital assets in regulated finance:

In 2025 the IOG engaged with existing Financial Market Infrastructures (FMIs), banks and their representative bodies to move the IOG and the Charter to the next phase. At our first face-to-face meeting in London in May 2025 the group agreed to start a grass roots project and create an organization provisionally named the **Interoperability Standards Organization for Digital Assets (I-SODA)**, to develop global interoperability standards for digital assets.

In this organization, systemically important FMIs, banks and asset managers, blockchains and their foundations, token solution providers, layer zero companies, bridge providers and other relevant actors will work together to publish neutral standards that can be followed by any entity that wants to tokenize a regulated asset.

Many participants have already created standards for this purpose, and I-SODA will not replicate any existing work or re-write existing token workflow specifications. I-SODA will act as a neutral host to abstract and harmonize existing standards, identify gaps in those standards and where needed, produce new technical standards for the tokenization workflow. This will enable regulated assets to flow from one digital eco-system to another, regardless of where the asset resides or which network is used to create the token.

I-SODA will be what is known in the United States of America as an SDO (a Standards Defining organization). The Internet Engineering Task Force (IETF) will provide the neutral framework for this organization to function. Previous examples of such neutral industry standards organizations hosted by the IETF include Secure Mail Transfer Protocol (SMTP) for email; Transmission Control Protocol/Internet Protocol (TCP/IP), for the internet; Trusted Computing Group (TCG) for semi-conductors; Open Identity Exchange (OIX) for identity verification, and many more. By following this model, MIT will be a neutral hosting body for I-SODA.

Looking at each asset class independently, the work of the organization will be divided into three distinct workstreams:

1. **The data model stream**: the information needed to define the asset and its life-cycle. This data definition resides outside all technology considerations, and creates the 'singleness' of an asset. Working through the collation and review of existing and proposed implementations, the data model will apply regardless of whether the asset is in digital or non-digital form.

2. **The common digital call functions stream**: a consistent framework that can be applied to smart contracts, or other forms of code, which enable the interaction with the asset. Regardless of the underlying blockchain or database, there will be common de minimis functions or action verbs which will be applied to all digital representations of a regulated asset. Some will be universal like 'mint' or 'burn', others will be dependent on the data model of the asset. This stream will also include the creation of a taxonomy for asset lifecycle participation and the role(s) played by the various participants and how they align with the data model.

3. **The legal and governance stream**: the regulatory frameworks which currently exist for assets in a non-blockchain habitat will be mapped and published to ensure legal and regulatory compliance. This will include elements such as legal role played by transaction participants, jurisdictional oversight and verification and identity requirements.

Today, we invite all token actors working in regulated finance to join us in developing interoperability standards:

- **Join the Interoperability Standards organization for Digital Assets (I-SODA) at MIT to help create the industry-wide call token standards for regulated finance**
- **Use the MIT and SODA Services team of experts to develop token standards for a specific use case**
- **Take part in the SODA 2026 tokenization benchmarking survey**

Section 2

Why are interoperability standards needed? Why now?

Tokenization can offer a series of benefits for global financial institutions as they undertake their activities in regulated finance. With a well-designed tokenization workflow, the benefits can include the removal of a single point of failure, greater transparency, faster settlement and improved cost and capital efficiency. The benefits of tokenization have indeed been felt by financial institutions as projects have matured throughout the 2020s, and many of these are covered by the practitioners themselves in section 3 of this paper.

These benefits, even when taken together, will only move the dial so far. With each 'successful' tokenization there is growing fragmentation, as tokens created on such divergent technologies create isolated pools of liquidity.

Ultimately, it makes little sense for financial institutions to tokenize more and more assets if micro-efficiencies lead to macro-inefficencies. The true macro-benefit of tokenized real world assets lie in a new global habitat which offers more liquidity and distribution than the current financial system ever will. A truly interoperable system of tokenization is one which allows an issuer and an investor to trade an asset on any technology at any time. Without such an interoparable habitat, tokenization will be limited to a series of channel-by-channel endeavors offering some improvements, but will never enable greater democratic access to the global financial system for more actors and new products, and the potential of a blockchain-based global financial system will not be fully realized.

As the history of the internet and the shipping container show us, if practitioners do not act now, while the industry is being formed, the opportunity to create a new financial system may be lost.

Interoperability lessons from history:

How the internet exceeded expectations

Thomas Hardjono

The success of the Internet can be measured by the sheer number of its users today, and by the various services and features that were not even conceived of when the TCP/IP protocol began to be defined in the mid-1970s. Today, billions of interactions occur daily over the Internet, with users located throughout the globe, seemingly unaware of the communications infrastructure making these interactions possible.

While the initial funding for ARPAnet – as the precursor of the Internet – was provided for the US Government, the understanding from its start was that the private sector would drive the further development of the civilian Internet and commercialize it. These private TCP/IP network providers became known as Internet Service Providers (ISPs). Another early realization was that IP data-packet delivery was only the base offering, and that higher-layer services, such as e-commerce and video-conferencing, would be built atop these base offerings.

Crucial to the success of the TCP/IP Internet was the early standardization of core building blocks that enabled the ISPs to interoperate and deliver IP data-packets that traverse over their networks. Examples of these standardized building blocks include the data-packet definition, local domain routing protocols, and the inter-domain gateway protocols that connect ISP networks. These standardization efforts primarily occurred within the Internet Engineering Task Force (IETF), an open-source standardization body. This effort subsequently expanded to other standard organizations, including the W3C, IEEE, and 3GPP.

One key aspect in the Internet engineering design was not to over-specify features, but to develop a layered architecture that enabled core functions (e.g. IP data-packet routing) to be defined at one layer and for other functions (e.g. user identity management) to be defined in the higher layers because these were not necessary for the goals of IP data-packet delivery end-to-end.

Another fundamental goal of the Internet engineering design in the IETF was to develop vendor-neutral specifications that anyone could implement free of royalty. This open philosophy enabled multiple competing vendors and ISPs to create offerings that could be tailored to different markets (e.g., home Internet, Enterprise market, Government market, mobile devices market). The overall goal was the same, namely, to connect users around the globe irrespective of where they are located geographically. Over time, these technical specifications continued to be updated as living specifications that evolved over the past three decades. Since numerous vendors, ISPs and users depended on these specifications – directly or indirectly – it was in their best interest to continue evolving these specifications following the same open philosophy.

The development of the Internet also spurred the creation of new physical infrastructures supporting digital communications. The "need for speed" in data-packet transfer invigorated the development of new fiber-optic technologies that would provide long-distance backbone connectivity, such as from one coast of the continent to another. These fiber-optic offerings expanded to undersea cable technologies that connected the continents of the globe. Router vendors, semiconductor manufacturers, and software vendors now had an expanded global market into which they could sell their products, which in turn funded new research into Internet technologies. E-commerce merchants could now sell goods to consumers located anywhere in the world, providing a boon for the transportation industry globally and for local goods delivery services.

One key lesson for the emerging tokenization industry today is that it is impossible to foresee what future commerce services could be developed atop a handful of basic, standardized building blocks for asset tokenization. Technical standards for tokenization should be blockchain-neutral and royalty-free, such that anyone can implement the standards over any blockchain system anywhere in the world with a high degree of interoperability. This would enable market competition for the best blockchain systems to be developed, focusing on satisfying market needs – which, in the case of tokenized assets, includes meeting regulatory compliance requirements.

Looking back 30 years, one can reasonably state that the TCP/IP Internet is probably one of the most significant technological advancements for human

communications, on par with the discovery of electricity (for the betterment of living) and the development of vaccines (for the betterment of human health).

The challenge for the tokenized assets community today is whether, in 30 years, one could look back and say that the tokenization of assets has provided a betterment in the economic conditions of humans around the world.

How the shipping container ushered in an era of globalization

Chris Ostrowski

In the 15th century the movement of goods by sea-borne vessels offered a pathway to prosperity through trade. The era of the Silk Road was replaced by an age of ocean-going ships that could carry bulk goods all over the world. Break-bulk shipping then continued up until the mid-20th century; more trade routes were opened and more ships were built with faster propellent technology as the centuries passed; maritime and commercial law matured, and humanity became ever-more prosperous despite the rise and fall of European Empires, World Wars and periodic regional conflict. Though a tonne of cargo could be shipped safely from one port to another with great efficiency, there was no globalisation in the trade of goods until the advent of the standardized shipping container – global trade became 'interoperable' from the 1970s and a new era of globalisation began.

Malcolm McLean, developer of the inter-modal shipping container. Photo courtesy of Wikipedia.

Extending this analogy to the world on web3 in the 2020s, the tokenization of real world assets also offers much promise and many greater efficiencies than the 'Silk Road' of the existing global financial system; web3 pioneers have demonstrated how tokenized assets can move safely from one from one blockchain technology to another. Companies have sprung up offering 'chain linking', and 'layer zero' bridging services to financial institutions which enable real world assets to move from existing databases to web3 habitats, and then also between blockchains, regardless of divergent and heterogeneous nature of the underlying technologies.

However, without standardised specifications and common market practises, the tokenization of real world assets will be limited to promoting single channel efficiencies – an asset class here for a bank, a new marketplace for some brokers there. Some token solution providers and blockchain eco-systems may offer their financial institution clients more liquidity and agility

than others, and each blockchain eco-system is already able to technically bridge with another blockchain eco-system, but this will never create an interoperable token habitat to deliver greater distribution and liquidity for the global financial system.

In the same way the inter-modal shipping container can move goods on a truck, a train or a ship anywhere in the world, by following a completely neutral common container standard, the Interoperability Standards Organization for Digital Assets will develop a standardized spec to enable any asset to be transacted on any technology – regardless of where the asset originally resides or where it is first tokenized.

Malcom McLean is credited with being the father of the shipping container. In the mid-20th century his fundamental insight which made the intermodal container possible was that the core business of the shipping industry "was moving cargo, not sailing ships with ever more efficiency." It took many lost decades before the industry practitioners came together, but when they finally did, a new era of globalisation began. In the same way we should see that the core business of fintech, and the token economy, is moving value to as many places and people as possible, not only improving market efficiencies with better technology.

1. Light Reading Website: "Malcolm McLean's fundamental insight, commonplace today but radical in the 1950s, was that the shipping industry's business was really cargo, not sailing ships," Finnie said, quoting from the book, The Box: How the Shipping Container Made the World Smaller and the World Economy Bigger.

Section 3

Articles from the SODA community

Those institutions that have actively participated in the MIT / SODA interoperability project were invited to contribute to this White Paper to show their support for this endeavor, and the vision outlined here-in. Many thanks to all those who have contributed to the White Paper and to those institutions which have acted observers and reviewers over the past few years.

Finding Common Ground with Diverse Technologies

LF DECENTRALIZED TRUST

Interoperability is a challenging problem in any context, and particularly in digital ones.

By definition, it is a problem where there are multiple stakeholders involved, each of whom probably believes that "their way" is the best way of doing things. Even in the best case, collaboration can be hard. To have the best chance at success, these collaborations must be open, neutral, and transparent.

Let's take a step back and look at the past. The internet was built on open and neutral protocols. Arguably the most important internet protocol, TCP/IP, has always acted as the "narrow waist" of internet traffi c: in other words, the interoperability layer.

Because TCP/IP is an open protocol, anyone can build on top of it without asking permission and, conversely, no individual or company can unilaterally make changes to it. This openness has been the key to migration to the internet as the global backbone for communications and commerce.

Meanwhile, AOL and other closed networks were short lived, despite early success. They were quickly eclipsed when both end users and companies were off ered the openness and innovation of a neutral, global internet.

That's just one example of the staying power of open technologies. Too often, the success of a project or standard rises and falls with a company or founder. New leaders or strategies or even political winds can implode a network or solution built on a centralized model.

However, protocols and standards that are developed, maintained and governed by a community are built for longevity. They continue to advance and evolve even as early contributors step aside, ensuring the long-term viability of the technology and its surrounding ecosystem.

This is not theoretical. While proprietary software and networks regularly hit a point where their market share fl attens or declines, neutral protocols such as TCP/IP, generally grow stronger as more participants adopt and improve them. It is not an accident that all of the leading standardization bodies, such as ISO, IETF, and W3C, consistently preach and enforce neutrality.

But neutrality and decentralized governance are not the only important requirements for standards governance. Transparency is critical. Trusted systems, such as financial and government networks, can't operate in the dark. They must operate with well-defined, verifi ed, and visible rules and standards to gain the confi dence of companies and consumers. Likewise, enterprises rightly are concerned about getting locked into a proprietary system or protocol that evolves without their input (or stagnates) and longer fits their needs.

Instead, they can opt for a more future ready approach by turning to openly developed and maintained technology and standards. Rather than vendor

lock, they have portability and the assurance of an open technology roadmap with transparent rules for shaping it. They aren't placing their trust in a single corporate entity but rather working with a community committed to the longevity and resilience of the technology and networks it powers.

So what can we do going forward? We need to develop standards for interoperability in open, neutral places, where everyone can participate. Like open source software, standards organizations should be governed as a "do-ocracy," where participants' voice in governance is strictly proportional to their contributions to the project. This creates a positive feedback loop that rewards participants for putting effort into a project.

We can emulate the open communities where mistrustful, competing institutions have come together to build lasting technology. Projects like the Linux kernel, Kubernetes, and the Apache server are all examples of such open communities. It is not a coincidence that both of their "host" organizations, the Linux Foundation and the Apache Software Foundation, enforce radical transparency and neutrality.

More recently, if we look at the blockchain community, at least some of the success of the Ethereum community can be attributed to the fact that there is not a single for-profi t company that controls the process, unlike many other popular blockchains. Since there are many diff erent implementations of Ethereum clients, almost all of which are developed outside of the Ethereum Foundation itself, the Ethereum Foundation can be thought of, at its core, as a standards organization: it helps facilitate setting the standard for the Ethereum protocol. The Ethereum Foundation enforces transparency and neutrality, and it is one of the core reasons why Ethereum technology is trusted and being adopted by so many institutions.

In summary, standardization efforts work best when standards projects are open, transparent, and neutral. In the case of interoperability, where there are almost necessarily mistrustful competitors that need to work together, these principles become essential.

Taking tokenization to the next stage

"We're at the beginning of the tokenization of all assets."
Larry Fink, BlackRock CEO

The opportunity is substantial. Analysts project that tokenized real-world assets could exceed $16 trillion in value by 2030, as payments, securities, and financial instruments move on-chain. If every asset class were ultimately tokenized, as Fink suggests, the total value of global financial assets could approach $867 trillion (World Economic Forum).

Market foundations are in place: mature Layer 1 networks, established token standards, growing regulatory clarity, and an increasing understanding of tokenization's efficiency gains. Yet institutional adoption remains limited by a persistent gap: **the absence of infrastructure that maximizes interoperability without compromising confidentiality.**

To move from largely internal deployments to an open network that delivers blockchain efficiencies at scale, institutions must be able to verify ownership, eligibility, and compliance without exposing commercially sensitive data.
SODA Labs – Interoperability Standards for Digital Assets White Paper 1

Achieving this balance, *programmable privacy within interoperable systems*, defines the next stage of tokenization.

About Applied Blockchain

Applied Blockchain has spent over a decade designing and delivering blockchain systems across finance, energy, and supply chains. Our work with leading institutions, including Shell, Bank of America, Barclays, and the United Nations, has consistently revealed that the barriers to scaling tokenization are not purely technical, they are also structural. **Interoperability, trust, and privacy** determine whether institutions can collaborate and transact securely across networks.

For regulated markets to adopt blockchain at scale, these elements must converge: shared standards for interoperability, and privacy mechanisms that protect commercial and compliance-sensitive data. This intersection defines Applied Blockchain's focus and ongoing technical innovation.

The Interoperability-Privacy Challenge

Ethereum has become the de facto standard for digital asset tokenization. Its token frameworks (ERC-20, ERC-3643) and development stack (EVM, Solidity) function as the HTTP, HTML, and JavaScript of blockchain infrastructure. Yet institutional adoption continues to stall at a familiar fault line: the trade-off between public transparency and private control.

Private and permissioned networks ensure compliance and confidentiality but isolate liquidity and restrict efficiency gains. Public networks enable composability and maximize efficiency gains but expose sensitive financial activity and participant identities.

True interoperability in regulated finance requires more than connecting ledgers; it requires **connecting trust**.

Regulation requires transparency and auditability, yet institutions must also protect commercially and legally sensitive information. **Without privacy, interoperability breaks down precisely where regulation begins.** This is not a technical limitation of blockchain; it is a design gap in how current standards and infrastructure handle confidential information.

This next generation of infrastructure must support both: true blockchain efficiency and commercial privacy.

Evolving Standards: Confidential Token Frameworks

ERC-20 is the most widely adopted token standard, with ERC-3643 gaining traction for regulated digital asset issuance. Both enable composability across EVM-compatible networks, forming the foundation of tokenized finance. Yet they were designed for transparency, not confidentiality: every balance, wallet address, and transaction detail is visible on-chain. This transparency supports auditability and verification but limits institutional and commercial use.

The next evolution is not a new standard but an extension; frameworks that preserve ERC compatibility and composability while embedding programmable privacy. This approach allows confidentiality to coexist with composability, preserving existing infrastructure while unlocking new use cases.

The next evolution is not a new standard but an extension; frameworks that preserve ERC compatibility and composability while embedding programmable privacy. This approach allows confidentiality to coexist with composability, preserving existing infrastructure while unlocking new use cases.

Applied Blockchain's Unopinionated Confidential ERC Framework (UCEF) exemplifies this model. Built with standard Solidity constructs, UCEF introduces privacy at the data level, allowing issuers and participants to control who can view balances, counterparties, or transaction metadata without altering the ERC-20 interface. As a result, UCEF remains fully composable with existing decentralized applications, wallets, and infrastructure.

Unlike other confidential token models that mandate a single cryptographic method, UCEF is cryptography-agnostic. Developers can integrate TEEs, ZKPs, or other privacy mechanisms depending on regulatory, performance, or security needs. This flexibility is critical in a multi-jurisdictional environment where compliance obligations vary and technology continues to evolve.

The same principles apply to UCEF-3643, Applied Blockchain's confidential implementation of the ERC-3643 standard used for compliant security tokens. UCEF-3643 combines identity-based permissions and regulatory controls with transaction-level privacy, concealing ownership and trade data from public view. In doing so, it demonstrates that compliance and confidentiality can reinforce, not oppose, one another.

These frameworks demonstrate that privacy and interoperability are not opposing forces. By maintaining compatibility with existing token standards, confidential frameworks allow institutions to adopt privacy-preserving capabilities without fragmenting liquidity or abandoning established infrastructure.

Evolving Infrastructure: Privacy-Enabled Layer 2s

Standards alone are insufficient. Scaling tokenization also requires infrastructure that supports privacy-preserving computation and verification at institutional throughput.

Layer 2 networks extend the capabilities of established Layer 1s, such as Ethereum, while offering flexibility in design and governance. Among them, **privacy-enabled Layer 2s** represent a critical evolution: infrastructure that enables secure computation and verification without exposing sensitive data.

Applied Blockchain's Silent Data illustrates this approach. It operates as a privacy-preserving Layer 2 built on the OP Stack, directly integrated with Ethereum. Rather than creating an isolated network, Silent Data extends the Ethereum ecosystem, inheriting its security, decentralization, and composability while adding a programmable privacy layer.

Silent Data uses Trusted Execution Environments (TEEs) and cryptographic attestations to enable sensitive data to be processed. Standard Solidity smart contracts can verify facts such as ownership, eligibility, or compliance status without revealing the underlying information. This approach **supports compliance** where regulation, privacy, and interoperability align.

TEEs offer distinct advantages in this context. Unlike zero-knowledge proofs (ZKPs), which can impose significant computational overhead and complexity, TEEs provide high performance and straightforward auditability. For regulated institutions, this matters: compliance teams and regulators can verify that computations **occurred correctly within a secure environment without requiring specialized cryptographic expertise.**

Silent Data also supports **selective disclosure** : participants can choose what information to reveal and to whom. An issuer might prove to a regulator that all token holders meet accreditation requirements without disclosing individual identities. A corporation might demonstrate compliance with transaction limits without revealing counterparty relationships or deal terms. This granularity is essential in environments where transparency to regulators must coexist with confidentiality in commercial relationships.

A Layer 1 network such as Ethereum provides a recovery mechanism for asset holders if a Layer 2 were to fail or become corrupted. This feature enables further compliance by reducing the onus of decentralized security on the Layer 2, enabling the Layer 2 network to be comprized of permissioned node validators.

As a privacy layer built on Ethereum, Silent Data complements the modular ecosystem of Layer 2s and rollups, extending their interoperability with privacy-preserving capabilities. It demonstrates how tokenization infrastructure can operate across networks while maintaining compliance, performance, and confidentiality.

Looking Ahead: Privacy as Standard, Not Feature

The internet scaled through open protocols that made connectivity a given rather than a challenge. Blockchain will scale through privacy-preserving interoperability standards that make trust verifiable across networks by default.

Privacy should not be treated as an optional add-on or a niche feature for specific use cases. It must become an intrinsic design principle, embedded in token standards, infrastructure, and governance frameworks. When privacy is a standard, interoperability follows naturally: institutions can connect, verify, and transact without the binary choice between openness and control.

Applied Blockchain's work on confidential token frameworks (UCEF, UCEF-3643) and privacy-enabled infrastructure (Silent Data) demonstrates how existing systems can evolve to meet institutional requirements without requiring wholesale replacement. The foundations – Ethereum, ERC standards, Layer 2 modularity – are sound. What remains is to extend them with privacy-preserving capabilities that operate at scale.

The next generation of tokenization will be defined by consolidation rather than dispersion of chains, connecting more securely, privately, and at scale.

That convergence – where standards, infrastructure, and privacy align – is already taking shape. The industry's task is to accelerate it, ensuring that technical foundations match the scale of the opportunity ahead.

Digital Assets in the Age of Tokenization: From Wrappers to Real Interoperability

Tokenization has been one of the most discussed promises of blockchain for nearly a decade. Yet if we are honest, much of what passes for tokenization today has been superficial. Most tokenized ETFs or deposit tokens function as wrappers: the enforceable legal claim remains with the custodian's traditional ledger, not with the token itself. The token provides digital exposure and settlement efficiency, but does not independently confer ownership rights. Bridging this gap, where the token itself is the legally binding claim, remains the challenge for the next generation of tokenization.

This is beginning to change. With emerging regulatory frameworks globally, the industry is gaining clarity about what can be done and how. This creates an opportunity and responsibility to rethink tokenization. Digital assets must move from wrappers to legally enforceable claims, from isolated silos to interoperable rails, from marketing exercises to industry standards.

What Needs to Be Tokenized

The financial system is made of concrete instruments, each with legal, operational, and data primitives that must be respected. Sovereign bonds, corporate debt, equities, money market funds, structured products, and bank deposits each carry specific disclosure obligations, identity requirements, risk models, and settlement rules. Yet they share fundamental primitives: ownership, transferability, finality, collateral eligibility, and regulatory oversight.

These shared primitives should be tokenization's starting point. Rather than creating bespoke tokens for each asset class, the industry should identify common elements, data fields, contractual hooks, compliance checks and build standards reflecting them. A sovereign bond and money market share may differ legally, but both require clarity of ownership, standard settlement instructions, and recognition in existing accounting frameworks. By focusing on shared foundations, we can create interoperable digital assets that plug into multiple systems without fragmentation.

Current Shortcomings and Ethereum's Response

Early experiments have proven appetite for tokenized products and efficiency gains from blockchain rails. But we must confront limitations. Private networks have demonstrated efficiency in silos that fail to interoperate with public infrastructure.

The Ethereum ecosystem has systematically addressed these challenges. Privacy, once considered blockchain's fundamental limitation, now has production-ready solutions through zero-knowledge proofs. Performance concerns have been addressed through Layer 2 scaling, with throughput expanding dramatically. While recent discussions around fast finality, performance, gas prediction and the Staking Approval Layers (SAL) from emerging L1 chains put the spotlight on some valid concern for adoption, Ethereum's roadmap is actively addressing this through ongoing research in

peer-to-peer networking and cryptography. (Ethereum 10k TPS in the next six months, PeerDas v2, Blobpool scaling for the more technical readers)

Ethereum is in 80 plus countries with 870,000 validators, 13,600 physical nodes, and millions of users across continents. The 10 years of continuous uptime and 16 successful network upgrades demonstrate not just technical capability, but something more important: the ability to evolve while maintaining stability. The Ethereum Foundation's technical stewardship has guided the network through fundamental changes without disruption: a critical requirement for financial infrastructure.

The challenges ahead aren't primarily technical. If we can build zero-knowledge proof circuits (among the most complex achievements in applied cryptography) we can solve the remaining technical requirements for tokenization. The real work is organizational: aligning standards, establishing legal frameworks, and coordinating across institutions. Without tokens that are themselves the legal claim, assets remain dependent on traditional infrastructure. Without interoperability, liquidity remains fragmented. Without standardization, regulators cannot oversee markets effectively.

A Methodical Approach

Moving forward requires starting from scratch, examining each asset class systematically to understand its requirements. This isn't about applying blockchain to existing structures, but understanding what each instrument fundamentally needs to function.

Consider the taxonomy work required: Government debt securities need issuer verification, maturity tracking, and coupon calculations. Money market funds require daily NAV calculations, liquidity management, and regulatory compliance reporting. Corporate bonds need covenant monitoring, credit rating updates, and payment waterfalls. Private credit demands tranche structures, default management, and cash flow modeling. Bank deposits require instant settlement, deposit insurance integration, and interbank connectivity.

Each instrument family shares base constructors, legal issuer, regulatory framework, ownership rights, custody arrangements, transfer restrictions, settlement mechanisms, yet implements them differently. A tokenized bond remains legally a bond, just with blockchain-based record-keeping. The work lies in mapping these requirements precisely:

Definition: What data must each asset class carry? Government bonds need ISIN codes and coupon rates. Private credit needs loan-to-value ratios and default provisions. This isn't theoretical. It requires working with issuers to understand exactly what information systems depend on.

Specification: How do we express these requirements in code?

Integration: How do these specifications connect with existing systems? A tokenized treasury must appear correctly in risk management systems expecting CUSIP codes. A tokenized deposit must integrate with payment networks expecting SWIFT messages.

This taxonomy and listing work, documenting every field, every calculation, every compliance requirement is painstaking but essential. Working groups like this one create the space for this detailed mapping across perspectives and disciplines.

Technical and Regulatory Progress

The Ethereum ecosystem's evolution demonstrates that technical foundations are being laid. Progress on token standards for regulated assets shows movement beyond simple implementations, the emergence of ERC3643 among other RWA standards has been showing great traction across the world.

The key is ensuring technical capabilities align with institutional requirements. Scalability matters only if it supports required transaction volumes. Privacy solutions matter for financial services only if they satisfy regulatory reporting. Interoperability matters only if it maintains legal and compliance properties across systems.

Technical progress coincides with increasing regulatory engagement. Policymakers globally are signaling readiness to provide frameworks for digital assets. Institutions can begin aligning digital asset strategies with emerging legal structures.

This matters because enforceability is the missing link. A token legally recognized as a share, bond, or deposit differs fundamentally from a synthetic wrapper. It's the difference between exposure and ownership.

From Wrappers to Real Assets

The question isn't whether we can put assets "on chain," but how we tokenize in ways that are legally binding, operationally compatible, and technically interoperable. This requires:

- Shared vocabularies and schemas for financial instruments
- Standards or middleware that captures legal claims and instrument-specific properties
- Integration with existing messaging and settlement systems
- Open, interoperable infrastructure avoiding silos

The solution might not require new token standards. ERC-20 with additional middleware, smart contract layers, or wallet-level implementations could provide the necessary distinctions. What matters is that the complete system, token plus supporting infrastructure, captures the legal and operational requirements of each instrument type.

Success means establishing common ground across implementations. Not every platform needs identical technology, but they must speak the same language when describing assets, transferring ownership, and reporting to regulators.

Meeting Institutions Where They Are

Institutions operate within constraints technology alone cannot ignore. Tokenization must work within these realities.

This means answering practical questions: How does a tokenized bond appear in risk systems? How do compliance teams monitor tokenized transactions? What happens during technical failures? Who bears liability for smart contract bugs?

The answers needn't be perfect, but must exist. Institutions need confidence that tokenized assets can be managed with the same rigor as traditional instruments, even while offering new capabilities.

Conclusion: A Concrete Example - Common Stock

To illustrate the work ahead, consider tokenizing something as fundamental as common stock shares in a publicly traded company like Microsoft.

Today's Reality: Data Across Multiple Systems

A single share of MSFT exists across numerous systems:

- **DTC (Depository Trust Company)**: Holds the master record of ownership
- **Transfer Agent (Computershare)**: Maintains shareholder registry with names, addresses, tax IDs
- **Broker Systems (Charles Schwab, Fidelity)**: Track customer positions, cost basis, purchase dates
- **Exchange Systems (NASDAQ)**: Record trading prices, volumes, order books

  Corporate Actions Systems: Process dividends ($0.75/quarter), stock splits, voting
- **Tax Systems**: Calculate withholding, generate 1099-DIVs, track wash sales
- **Regulatory Reporting**: File 13F holdings, insider transactions, short interest

Each system holds different pieces: ownership (who), economics (dividends, price), rights (voting), compliance (restrictions), and operations (settlement).

As a Token: What Data Goes Where?

The token itself might contain:

- Symbol: MSFT
- Total shares outstanding: 7.43 billion
- Current holder address: 0x742d35Cc6634C053...
- Balance: 100 shares

But where does everything else live?

- **Shareholder identity**: On-chain privacy is required, but regulators need visibility
- **Voting rights**: How do 100 tokens know about an upcoming proxy vote?
- **Dividend entitlement**: Who tracks record dates and payment calculations?
- **Trading restrictions**: How are insider lockups or Rule 144 limits enforced?
- **Corporate actions**: If Microsoft splits 2:1, who updates 100 tokens to 200?
- **Tax basis**: Purchase price and date for capital gains calculations
- **Beneficial ownership**: If held by a custodian, who's the real owner?

Now just looking at trading restrictions: When an executive violates their lockup agreement by transferring tokens through a DEX, how do we enforce the SEC settlement agreement that requires disgorgement of profits?

The executive's tokens are locked, but then what happens:

1. **They create a synthetic position** – They borrow against their locked tokens on Aave, sell the borrowed assets, effectively getting liquidity without moving their tokens. Is this a violation? The tokens didn't move, but they achieved the economic effect of selling.

2. **They use a wrapper protocol** – A DeFi protocol creates derivative tokens backed by their locked shares. They sell the derivatives. The original tokens never moved. Did they violate the lockup?
3. **The lockup expires incorrectly** – The smart contract has a bug or someone set the wrong date. Tokens unlock 30 days early. The executive sells. They claim they acted in good faith. Who's liable?
4. **Cross-chain complexity** – Their tokens are locked on Ethereum, but they bridge representations to another chain where the restrictions don't apply. Which chain's rules matter?
5. **Legal dispute** – The SEC says the executive had material non-public information. The executive says they didn't. The court orders disgorgement. The tokens already went through Tornado Cash. Now what?

These aren't technology problems, they're design decisions requiring securities lawyers, transfer agents, tax specialists, compliance officers, and technologists working together. Each answer affects whether institutions can legally hold these tokens, whether markets can efficiently price them, and whether regulators can effectively oversee them.

This methodical mapping, asset by asset, field by field, system by system, is the real work of tokenization. Not the technology, but understanding what needs to be built.

We are heading towards a world where purchasing and trading financial instruments are as easy as online shopping.

This future is powered by the tokenization of real-world assets (RWAs). Analysts estimate that tokenizing RWAs could unlock **$400 billion in additional annual value across** the financial value chain and hit a **market cap of $2 trillion by 2030**. It's seen as the third wave of asset management innovation, unlocking global access in ways once thought impossible.

Tokenized RWAs have to be permissioned

To achieve benefits tokenization promises, asset owners have to ensure the legal link between the tokens and the underlying assets they represent on the blockchain. For this, wrapping the asset in a financial product and using on-chain identities is key. Tokens must be technically advanced enough to verify the identity of the token holder when they are transferred, to guarantee a real transfer of ownership of the underlying assets. In most jurisdictions, fractionalizing RWAs such as real estate, fine art or fine wine often make them fall into the scope of financial products.

In some cases, issuers must set up a Special Purpose Vehicle (SPV) to legally hold the underlying asset, and then tokenize the shares of that SPV. From there, the tokens are subject to the same securities laws as their traditional counterparts, with investor eligibility, transfer restrictions, reporting obligations, and jurisdictional limits, etc. These compliance constraints come with benefits, mostly providing guarantees to investors.

This is where the challenge lies. Tokenized RWAs have to enforce the same securities laws throughout the entire lifecycle of the tokens. Unlike cryptocurrencies, which can be freely traded by anyone anywhere, tokenized RWAs have to be permissioned to control who can access tokens and when tokens can be transferred.

Permissioning without interoperability leads to silos

In the past few years, the market participants have created solutions to applying permissions at blockchain level and platform level to enforce compliance, however it limits the interoperability which risks creating silos as well as single points of failures.

Private permissioned blockchains

In the early stage of tokenization, institutions launched private permissioned networks to control access. These closed environments worked as safe testbeds but offered little interoperability. Each system was an island, with individual integration rules and no way to connect to the broader DeFi ecosystem. As a result, some drew the wrong conclusion that blockchain's benefits were overstated. In reality, blockchain's true value lies in interoperability, when tokens themselves carry compliance and can seamlessly interact across platforms and networks.

Public permissionless blockchains with wallet whitelisting

As the industry progressed, some companies attempted to use public blockchains by adding wallet whitelisting to the ERC-20 standard, a very light form of permissioned tokens. In this model, if a wallet address is on the static whitelist, it can hold the tokens.

The main problem with this approach is that wallet whitelisting places all critical controls at the platform level. On-chain, the blockchain only recognizes wallet addresses, not investors' identities. The actual investor registry is maintained off-chain in the platform's database. This creates a fundamental weakness: the platform becomes a single point of failure.

If the platform is unavailable or compromised, the link between wallets and investors is lost. The tokens cannot serve as a reliable source of truth, because compliance is not validated on-chain but enforced through a static off-chain checklist. In such a setup, issuers and regulators cannot rely on the blockchain as the golden registry of ownership.

For financial institutions, this architecture undermines the core value of tokenization: resilience, transparency, and interoperability. Instead of reducing reliance on intermediaries, wallet whitelisting increases operational risk and confines assets within fragile, siloed systems.

Onchain Identity Unlocks Interoperability and Compliance

The alternative is to couple permissioned tokens with onchain identity. Instead of relying on static lists, investors are linked to identity contracts that store dynamic proofs, called claims. For example, that an investor is KYC-verified, accredited, or resident in a specific jurisdiction.

When a transfer is attempted, the token queries these claims directly onchain to confirm eligibility. In this model, the smart contract automates the platform's role in the wallet whitelisting model. It validates the actual compliance rules itself, instead of just checking whether a wallet address appears on a whitelist.

This shifts the golden record from the platform's database to the blockchain, removing the single point of failure and enabling assets to interoperate seamlessly across platforms, custodians, and distribution channels.

The Need for a Common Language: ERC-3643

Across the markets, there are many different ways to design compliance frameworks with digital identities. Without a shared approach, each institution builds permissioned tokens in its own way, leading to fragmentation and incompatibility.

This is why standardization is essential. ERC-3643 (also known as the T-REX Protocol), built on top of the ERC-20 standard, provides that common language. Originally created by Tokeny in 2018, it is now an official ERC standard and widely recognized as the market standard for compliant tokenization.

Its credibility is reinforced by more than 130 industry members, including DTCC, Apex Group, Invesco, and ABN AMRO, through the non-profit ERC3643 Association. It has been recognized in reports by large institutions and authorities such as Citi, **J.P. Morgan**, **BCG**, **ESMA**, and **MAS's Project Guardian**, and **World Economic Forum**. Most recently, SEC Chairman Paul S. Atkins cited ERC-3643 in his speech announcing **Project Crypto**, as an example of how compliance can be enforced directly on tokenized assets.

ERC-3643 provides a standardized framework that allows issuers to embed investor rules and transfer rules directly into tokens. Each transaction can only be triggered when all compliance rules are met throughout the lifecycle of ERC-3643 tokens, ensuring always-on compliance.

ERC-3643 is the standard that gives the industry a solid base to truly build on. Investor eligibility is validated through on-chain identity smart contracts, where claims, such as KYC approval, residency, or accreditation, are issued and maintained by appointed agents.

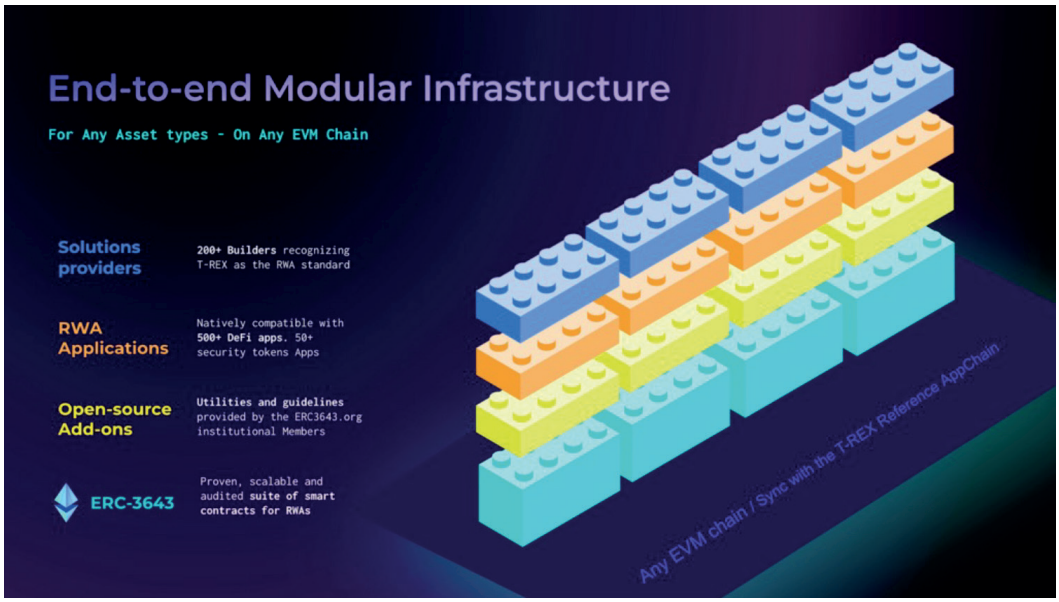
When a transfer is triggered, the ERC-3643 token automatically checks whether the investor's identity holds the required claims, issued by a trusted entity and if they are still valid (claims can lose validity under different circumstances). For example, if an investor failed to provide an updated proof of residence, the issuer or its appointed agent can revoke its residency proof, the transfer will be blocked. This ensures a dynamic, real-time eligibility check at every step with up-to-date compliance information.

On top of that, ERC-3643 is modular and flexible. Issuers can add any compliance rule they need, from limits on daily transfers to caps on investors per jurisdiction.

Rules can also be updated at any time to meet new regulations or regulatory updates. This adaptability makes it possible to align with regulatory requirements in any market. ERC3643 smart contracts use a proxy contract called 'Implementation Authority' to delegate its logic to an implementation contract, so it can be 'upgraded' by pointing to a new implementation contract.

To update the smart contract, the owner can set the address of the new version of the implementation contract, and the token will adopt the new logic of this contract. Furthermore, multi-token issuers can point all tokens to the same Implementation Authority contract so that upgrades are automatically applied to all their tokens simultaneously.

Finally, ERC-3643 is fully composable because it is built directly on ERC-20. It adds a compliance layer on top, while remaining natively compatible with every ERC-20 tool, wallet, and application. Developers can reuse existing modules and tap into the vast ERC-20 ecosystem, achieving the same network effects but with compliance embedded. Unlike other security token standards that created non-compatible interfaces and struggled with adoption, ERC-3643 scales seamlessly with today's infrastructure and tomorrow's innovations.



ERC-3643 Brings Interoperability for EVM and Non-EVM Networks

As tokenization expands, operational fragmentation is emerging as one of the industry's greatest challenges. Institutions are deploying assets across multiple blockchains, some EVM-based, others non-EVM. Service providers,

custodians, and administrators are expected to integrate with all of them, but each new setup adds complexity and cost.

Without a common compliance standard, every network risks designing its own method to validate eligibility and enforce rules. This leads to more fragmentation, forcing operators to spend time and resources analyzing, interpreting, and adapting to each unique framework before they can service assets smoothly.

While EVM chains can adopt ERC-3643 directly, non-EVM chains can mirror the framework to create their own version of the T-REX standard in their native language. By applying the same compliance model across all environments, service providers and applications gain a consistent way to operate tokenized RWAs, making integration faster, easier, and more reliable. The business logic and technical rules stay aligned, no matter which blockchain is used.

This alignment prevents the market from fragmenting into silos and enables a truly interoperable tokenization economy, where assets, applications, and service providers all operate under the same compliance language.

The ERC-3643 Association has already welcomed non-EVM ecosystems such as Stellar, Solana, and Movement, supporting them in mirroring ERC-3643 and building their own T-REX standards.

The future of real-world asset tokenization will be interoperable, compliant, and global.

A Call to Build the Future of Tokenization

The call to action is clear. For developers, ERC-3643 is a foundation to build on, enabling new applications and reusable modules that can scale across the entire market. For issuers, it is the safer path: adopting the standard ensures interoperability and avoids the risk of building isolated solutions that lock assets into silos. And for regulators, ERC-3643 provides a framework that aligns technology with existing rules, preventing overregulation while even creating room to modernize.

ERC-3643 is more than a standard, it is the backbone of a compliant, interoperable, and future-ready tokenization ecosystem. We invite the industry to join us and build on it.

A Common Approach to Standardize Tokenization

Every major advance in financial systems has come from standardization. SWIFT unified how banks communicate. ISINs standardized the identity of securities. LEIs created a shared format for institutional entities.

In digital assets, the same transformation is underway. LayerZero's OFT (Omnichain Fungible Token) Standard defines a common message format for how value and state move between blockchains – creating the first universal solution for tokenized assets.

Unlike early token standards such as ERC-20, which established uniformity within a single blockchain, the OFT Standard extends that logic across all blockchains. It defines a universal message packet that can represent any on-chain instruction—whether a payment, a token transfer, or a state update – enabling digital assets to move freely between ecosystems while remaining under issuer control.

Today, the OFT Standard is the most widely adopted framework for cross-chain tokenization and value transfer. It supports more than 500 tokens, representing over $90 billion in assets across 150+ blockchains, with over $100 billion in cumulative transfers. Every message follows the same schema, allowing value to move across blockchains the way data packets move across the internet.

Two architectural pillars define this system:

1. **Universal Packet Construction Across Ledgers**
2. **Isolated Security Owned by Asset Issuers**

Universal Packet Construction Across Ledgers

Earlier standards—ERC-20 on Ethereum, SPL on Solana, and the Move Coin module on Aptos and Sui—created local consistency but not interoperability. Each blockchain remained a closed network with isolated liquidity.

The OFT Standard resolves this by defining a common smart contract interface that encodes and decodes cross-ledger instructions using a standardized packet format. Each OFT contract acts as a "translator," interpreting commands such as mint, burn, and transfer through the LayerZero messaging protocol.

In practice, when an OFT token moves from one blockchain to another, no wrapped or synthetic asset is created. The token supply is burned on the source chain and minted on the destination chain under the issuer's authority. This direct supply migration preserves fungibility, prevents fragmentation, and maintains a single canonical asset across all connected chains. It also enables assets to move between separate blockchains 1:1, with zero slippage.

To visualize:

> If 10 PYUSD move from Ethereum to Solana, the Ethereum contract burns 10 tokens, sends a message packet via LayerZero, and the Solana contract mints 10 tokens once verification completes.

LayerZero itself functions as neutral message transport—similar to how TCP/IP moves packets across the internet. It does not hold keys or custody of any assets. Asset issuers retain full control of token supply, private keys, and issuance logic, while LayerZero provides the standardized channel for cross-chain communication.

Examples of live adoption include:

- State of Wyoming: issues the Wyoming Stable Token (FRNT) on seven blockchains while retaining full reserve custody and control.
- PayPal (PYUSD): issued by Paxos, connects its stablecoin contracts for PYUSD across Ethereum, Arbitrum, and Solana using the OFT framework.

Isolated Security Owned by Asset Issuers

Connectivity alone is not sufficient. Each cross-chain message must be verified under security assumptions defined by the entity that issues or operates the asset. LayerZero enables this through Decentralized Verifier Networks (DVNs), a modular security model that allows every application or issuer to decide who verifies its messages and how.

Each cross-chain message is attested by the issuer's chosen X-of-Y-of-N configuration—specifying how many independent verifiers must confirm a message before it finalizes. This design allows an issuer to tailor verification to its regulatory, operational, or risk profile.

DVNs operate as independent verification networks, each responsible for confirming the validity of messages sent through the LayerZero protocol. They function much like distributed auditors: rather than relying on one shared validator set, each application or issuer chooses its own set of verifiers. More than 50 DVN operators already exist, including:

- Enterprise providers: Google Cloud, Deutsche Telekom
- zk-proof systems: Polyhedra zkBridge
- Tokenization operators: BitGo, Paxos

Multiple DVNs can be assigned to the same transaction, providing redundancy and fault tolerance. If one DVN experiences downtime, latency, or even a compromise, the others continue to attest to message validity. Because each application defines and operates within its own isolated DVN configuration, security risks do not cascade across the ecosystem.

In practical terms, if an issue occurs within the DVN of one asset—say, a stablecoin—the event has no impact on other assets using separate DVNs. This isolation of trust ensures that no single point of failure can compromise LayerZero's network integrity.

This modular structure not only decentralizes security but also introduces programmable security. Institutions can embed asset-specific or jurisdiction-specific rules directly into verification logic—for example:

- **Compliance controls:** DVNs can enforce rate limits, whitelists, AML, sanctions, or jurisdictional screening at the message-validation layer.

- **Custom validation:** requires that an issuer-owned DVN running internal compliance logic for each transaction approves a message before execution.
- **Regulatory alignment:** implement DVNs that verify compliance with frameworks like MiCA or NYDFS before finalizing transactions.

Conclusion: Standardization as the Foundation of Tokenized Finance

The OFT Standard defines a unified architecture for tokenization—connecting assets across more than 150 blockchains while preserving issuer control over security and verification.

Because it is neutral, open, and programmable, the OFT framework supports multiple tokenization models within a single structure. Stablecoins, deposit tokens, tokenized treasuries, real-world assets, equities, and yield-bearing instruments can all be issued, verified, and settled across networks through a common protocol.

By standardizing message packets and allowing issuers to retain full sovereignty over their keys and verification logic, the OFT Standard establishes the foundation for a borderless, programmable, and verifiable financial system—one in which value moves as freely as information, and every ledger speaks the same language.

Tokenization: how FMIs can help facilitate an interoperable future

Fireblocks

Blockchain and digital assets represent the biggest disruption to traditional financial institutions in decades. But the most innovative Financial Market Infrastructures (FMIs) see things differently. Whether they are an exchange, a central counterparty (CCP), a payments system, or a central securities depository (CSD), they recognize that FMIs have a crucial role to play in coordinating the market and catalyzing the safe adoption of digital assets to support a more effective financial system.

And this role becomes increasingly more important as digital asset adoption continues. To date, we've seen these adoption trends happening in three distinct waves, each laying the groundwork for the next:

1. The adoption of crypto helped prove out the technology and improve the infrastructure and security.
2. The more recent swell in stablecoin usage has demonstrated the utility value of moving money in real time.
3. This in turn has set the stage for the tokenization of financial and real world assets.

Around $300 billion worth of money and assets has already been tokenized, providing a clear foundation from which this market is set to expand. Based on our research with clients, industry participants and partners, we estimate that the total value of tokenized money, funds, bonds, alternatives and equities on blockchains will reach $5 trillion by 2030.

- Tokenized asset market in 2023 alt assets, equities, funds, bonds, money, crypto

This new paradigm will not materialize overnight. It will build gradually, with different markets maturing at different speeds, reflecting the overall improvements on revenues and costs benefits that tokenization delivers, but also the market dynamics as those benefits affect different parts of the value chain.

First will be the simplest and most liquid markets: money and funds. These are the instruments where tokenization is already taking hold, because they have the clearest business case with immediate returns and are supported by infrastructure that is ready to absorb them. By creating the foundation of liquidity and trust, they set the standards that will shape everything that follows.

As that foundation is established, tokenization will extend into less liquid markets. Bonds, commodities, and real estate are being explored and will add the next layer of scale. Equities are now also being tested in tokenized form, seeking to offer 24/7 trading and seamless settlement against tokenized money. As they mature, each market will build trust, improve standards and help reinforce the next, laying the groundwork for broader adoption and higher volumes. FMIs will be critical at each stage, ensuring interoperability, trust and systemic resilience as tokenization moves deeper into financial markets.

- Tokenized Funds: Unlocking Efficiency in Money Market and ETF Infrastructure

Following closely behind tokenized money, funds are proving to be one of the earliest institutional use cases for tokenization. The business case is straightforward: money market funds and ETFs are highly liquid, widely used, and benefit immediately from the efficiencies of blockchain infrastructure. Issuers can streamline distribution, settlement can occur in near real-time, and investors gain greater transparency into fund flows.

Compared to stablecoins, tokenized money market funds offer yield to their holders and have already gained traction in digital asset markets. They can be used as collateral at exchanges to fund trading activity, while also generating yield for the holder. The clearest example is BlackRock's launch of BUIDL, its first tokenized money market fund, on Ethereum. Securitize acted as transfer agent, tokenization platform, and placement agent, relying on Fireblocks key management to secure the smart contracts, including to issue and burn the tokens. This partnership between the world's largest asset manager, a leading tokenization platform, and Fireblocks shows how mainstream funds can be digitized on public blockchains while meeting institutional standards for trust and security.

Other fund managers are following suit. Franklin Templeton's on-chain government money fund was the first US-registered mutual fund to operate on a public blockchain, now available on both Stellar and Polygon. These examples demonstrate that fund tokenization has already moved from pilot projects into production.

By 2030, we expect tokenized funds to account for around $1 trillion. Exchanges and CSDs can play a central role in scaling this adoption by providing trusted custody and distribution infrastructure, ensuring compliance frameworks are met, and supporting interoperability between fund platforms and broader market infrastructure.

- How Tokenization Is Reshaping the Bond and Loan Ecosystem

Fixed income markets may have the most to gain from tokenization. The global bond market is vast, and its settlement infrastructure is complex and costly. Tokenization can simplify this dramatically by enabling atomic delivery-versus-payment, streamlining processes, eliminating reconciliation errors, and reducing counterparty risk. For issuers, it offers efficiency. For investors, it can broaden access and create faster, safer settlement.

As an example, ABN AMRO has led the way in Europe by issuing a number of tokenized corporate bonds, exploring how companies can raise capital effectively onchain. These examples showed that the technology can support the use case, but also revealed the challenges in attaining critical mass required to migrate such a well-established market to new infrastructure.

Project Eden showed how FMIs can serve as a catalyst by convening 12 of the world's largest banks to participate in the issuance of a digital government bond on the Tel Aviv Stock Exchange. Bids were submitted through Bloomberg terminals, as in any traditional auction, but issuance, tokenization, and settlement all took place on-chain. Fireblocks provided the secure infrastructure for minting the tokens and enabling atomic delivery-versus-payment. The result was a proof point that tokenized bonds can integrate seamlessly with existing market practices while removing reconciliation costs, reducing settlement risk, and paving the way for future interoperability with CBDCs.

Given the speed and programmability of digital asset markets, we have seen increased demand for short-term lending, including repurchase agreements (repos). Broadridge's tokenized repo market, for example, has reached impressive scale and we are starting to see increased appetite for intra-day repos—something largely unattainable by the traditional financial system, made possible by the programmability and instant settlement of digital assets.

By 2030, we expect tokenized bonds, loans, and repos to represent around $1.3 trillion. FMIs are uniquely placed to lead here, given their experience in coordinating large-scale change. Just as DTCC orchestrated the transition to T+1 settlement in the United States, FMIs can set the standards and provide the infrastructure needed to ensure that tokenized fixed income markets are resilient, interoperable, and trusted.

- Bringing Private Markets OnChain: The Tokenization of Alternatives

Alternative assets represent one of the largest opportunities for tokenization. This category of tokenized real-world assets includes real estate, private equity, venture capital, and commodities, with a combined market value of over $570 trillion. Yet access to these assets is typically limited to large institutions and ultra-high-net-worth investors, with distribution constrained by illiquidity and high minimum investment thresholds.

Tokenization offers a way to change that. By enabling fractional ownership, it can open up exposure to a broader range of investors while also improving liquidity and transparency. Tokenized real estate in Asia and on-chain venture funds in Europe are early signs of this shift. These initiatives remain small in scale, but they demonstrate how blockchain infrastructure can support new models of distribution for asset classes that have historically been locked away.

By 2030, we expect tokenized alternatives to account for around $400 billion. FMIs will have an especially important role to play as less liquid, harder-to-value assets require consistent standards, trusted custody, and strong governance frameworks to ensure investor protection. FMIs are well placed to provide the sandboxes, interoperability, and systemic trust that will allow alternative assets to move from niche pilots into mainstream adoption.

- Why FMIs Are Essential to the Future of Tokenized Financial Markets

FMIs bring the trust, governance, and systemic resilience that are essential for tokenization to scale. Fragmented standards and interoperability gaps remain major barriers, and FMIs have the credibility and convening power to resolve them. Their track record in coordinating large-scale change shows why they are indispensable in this era.

The tokenization wave is advancing quickly. FMIs can either adapt to it or lead it. Those that lead will embed their standards and resilience at the heart of tomorrow's markets, ensuring tokenization develops into a safer, more efficient, and more inclusive financial system.

Seamless Interoperability in a Multi-Chain Future

One of the most exciting frontiers in digital asset infrastructure is interoperability: the ability for assets and data to move securely and instantly across different blockchains that serve different purposes. That is, if you believe in a seamlessly connected multi-chain world, like we do.

At Matter Labs, the team behind ZKsync, we view interoperability not as an optional feature, but as a native property of the protocol. It is what allows many private and public layer 2s, each either run by separate entities or serving different purposes in different regions, to exist in parallel and be connected, while the end-user experiences simplicity, speed, and security.

ZKsync uses Zero Knowledge (ZK) cryptography to scale Ethereum and allows for many layer 2s to be spun up and connected to scale the ecosystem, just like we spin up servers to scale the internet without restrictions. It allows for example for financial enterprises to control their own private and permissioned blockchain instance and keep data within their cloud or on premise, while still benefiting from the benefits Ethereum has to offer.

One-Second Interoperability Across ZKsync Chains

Within the ZKsync ecosystem, interoperability has been designed at the protocol layer. This means that all ZKsync instances (whether public chains or private deployments known as Prividiums) are natively connected. The result: transactions can flow from one chain to another in about one second, with final settlement secured by Ethereum.

Take a simple example. A user holds tokens on Chain A but wants to swap them for another asset that is only liquid on a decentralized exchange hosted on Chain B. Traditionally, this would require bridging, wrapping, or navigating multiple interfaces, which are slow and often risky steps.

With ZKsync's Interop, the process becomes seamless:

- The user initiates the swap from their account on Chain A.
- Behind the scenes the asset on Chain A is moved to Chain B where it is swapped for the desired asset.
- That asset is moved back to Chain A completing the transaction.
- The user experiences this as a single, near-instant transaction.

In other words: a multi-chain operation that feels like a single-chain operation.

This is not just a technical convenience. It is a redefinition of user experience. It means that banks, asset managers, or corporates adopting tokenized finance can interact across specialized environments (eg payment chains, trading chains, custody chains) without their clients or employees ever realizing they are crossing infrastructure boundaries. Every instance (or chain) is able to whitelist other chains they're comfortable interacting with after having done the required risk - and compliance checks.

Security by Design

The foundation of this interoperability lies in ZK proof technology. Each transaction is secured by a ZK proof that verifies its integrity. These proofs are aggregated via the ZKsync Gateway, which coordinates communication between chains while reducing costs. The process eliminates the need to rely on capital inefficient "bridges" or intermediaries.

This architecture achieves three critical goals for institutions:

- Speed: Proofs are generated and verified fast enough to support near-instant transfers.
- Security: Every step is cryptographically validated, anchored to Ethereum for finality.
- Scalability: Multiple chains can interoperate without fragmenting liquidity, since they share a common proof infrastructure and because it is possible to aggregate thousands of ZK proofs into 1 single, equally secure ZK proof for verification on Ethereum.

The result is interoperability that is both practical for end-users and robust for institutions and regulators.

The Coming Multi-Chain World

Looking ahead, we believe the digital asset landscape will not converge on a single chain. Instead, we will see a number of major blockchains, fully interoperable, each optimized for different use cases and audiences.

This is not unlike how we all use multiple email addresses today. We all have a work email, an Outlook account, and a Gmail account. Each serves a distinct purpose, and we switch between them effortlessly. The same will be true for blockchains. One may be optimized for regulated finance, another for consumer applications, another for global payments. The key is that they are seamlessly connected, so users move across them without friction or risk.

Just as the internet did not collapse into one network provider, digital assets will thrive in an ecosystem of specialized but interoperable platforms.

Interoperability as the Enabler of Scale

For tokenization to fulfill its promises of global liquidity, instant settlement and programmable finance, it must operate across borders, systems, and networks. For this we require a shared set of standards for digital asset interoperability.

Thanks to its customisability and composability, ZKsync's technology is suited to be the financial blockchain infrastructure of choice and any set of standards institutions decide to adopt to allow for efficient interoperability can be implemented. Just like ISO standards are required for exchange of payment messages and data between financial institutions today.

This is the foundation for a financial system that is both open and resilient. And it opens the door to a future where digital assets flow as freely and as imperceptibly as information does across the internet.

Unlocking Institutional Tokenization at Scale With an End-to-End Interoperability Standard

As tokenized assets continue to get issued across hundreds of disconnected public and private blockchains, it's essential that these assets can seamlessly move across chains in the same way that data moves across computers today.

However, transferring an asset across different blockchains is just the first interoperability challenge institutions must address. Institutions also need to ensure that all of the critical data underpinning the asset stays synchronized and up-to-date as the asset moves across chains, such as NAV data, Proof of Reserve, corporate actions events, and more. Additionally, in order to transact with blockchain-based assets, institutions need a way to connect their trusted in-house infrastructure to blockchains using established messaging standards. Then, whether performing investor accreditation checks to verifying transaction limits, institutions also need to ensure their privacy and compliance systems are connected to blockchain workflows to meet consumer and regulatory requirements.

Recent discussions at Swift's Sibos conference have reinforced this point: true interoperability must unify digital assets, payment rails, and institutional systems into one programmable fabric. Without an end-to-end interoperability standard, there will continue to be liquidity silos and system fragmentation, and the costs, complexities, and development timelines of adopting tokenized assets will remain prohibitive for financial institutions.

Therefore, establishing a universal standard for end-to-end interoperability is critical to the success of institutional tokenization on a global scale. Such a standard must not only support cross-chain functionality, but do so at the highest levels of security and reliability while also enabling key data, compliance, privacy, and existing system connectivity requirements to be met directly in the interoperability layer.

Cross-Chain Interoperability

Hundreds of public and private blockchains now operate in parallel, each with unique standards, finality assumptions, governance models, and compliance rules. The result is isolated liquidity pools, disconnected applications, and duplicate asset versions, making it extremely difficult to operate securely and efficiently at any scale.

The current multichain landscape resembles the pre-TCP/IP internet where networks were unable to interoperate, forcing every connection between networks to be customized and built from scratch. Without a common blockchain interoperability standard, there will be a growing list of bespoke bridging solutions, each introducing their own unique trust assumptions and security risks that institutions have to spend time and resources understanding and integrating before implementing their core business logic.

For the multi-chain ecosystem to operate at scale, blockchains must have a shared and open interoperability standard, one built on a secure and reliable foundation and supports key cross-chain functionalities. To that end, interoperability solutions that enable cross-chain token transfers and messages are important, but chain-to-chain interoperability is just the starting point. Institutions also need an interoperability solution that ensures data is is synchronized as it moves across chains. Creating a shared layer for data and value to move across the onchain economy not only enables liquidity to move to where there's demand, but it also enables assets and applications to be managed across networks securely, efficiently, and in real-time.

Existing System Interoperability

The current global financial system is underpinned by core infrastructure that is proven to secure trillions in value daily, hardened by decades of testing, regulation, and operational excellence. This existing infrastructure is not obsolete, rather it is indispensable, and core to key processes used by market participants like custodians, transfer agents, fund administrators, payment systems, CSDs, and more.

The goal of tokenized finance should not be to replicate or replace all of these trusted systems, but instead integrate them directly with blockchains in a secure and standardized way. However, the key challenge is that these systems were never designed for blockchain connectivity, meaning institutions have had to rely on many different custom/bespoke integrations to get blockchain-connected, many of which are resource-intensive and prone to delays and errors.

Having an end-to-end interoperability standard that extends beyond cross-chain communication to also define how offchain systems—banking infrastructure, data providers, enterprise platforms, web APIs, etc.—directly integrate with onchain systems would create a universal standard for operations across global finance more broadly. This would accelerate the adoption of tokenization within existing capital markets and establish a common framework for how the majority of tokenized asset transactions will occur as a hybrid set of onchain and offchain components. Thus, interoperability standards should also be capable of acting as a standardized orchestration layer for coordinating workflows across legacy infrastructure and blockchains.

End-to-End Interoperability

Beyond connectivity across chains and existing systems, an end-to-end interoperability standard must also embed the key building blocks necessary for powering tokenized asset transactions, namely data, compliance, privacy, and orchestration.

Just like in the traditional financial world, almost all onchain transactions will need some type of data, whether that isNAV, AUM, KYC/AML, as well as embedded compliance policies and conditions that must be met for the transaction to be approved. This can range from identity and investor accreditation requirements to internal business rules around transaction limits and operating hours. Furthermore, many transactions will need some form of privacy to meet consumer and regulatory requirements. As a result, an interoperability standard can only truly take off if it also supports the essential components that most advanced transactions beyond simple payments require.

Chainlink: The End-to-End Interoperability Standard

Chainlink solves all of the interoperability challenges for institutions as it is the global standard unifying disparate blockchain networks and existing systems with all of the key data, cross-chain, compliance, privacy, and orchestration needed for advanced blockchain transactions. As the only oracle platform to achieve **ISO 27001 & SOC 2 compliance**, Chainlink delivers unparalleled security and reliability and currently secures over $100 billion and powers the majority of DeFi markets. Chainlink's industry-standard oracle platform has also enabled tens of trillions of dollars in onchain transaction value, and many of the world's largest financial services institutions have adopted Chainlink's standards and infrastructure, including Swift, Mastercard, Euroclear, and many others.

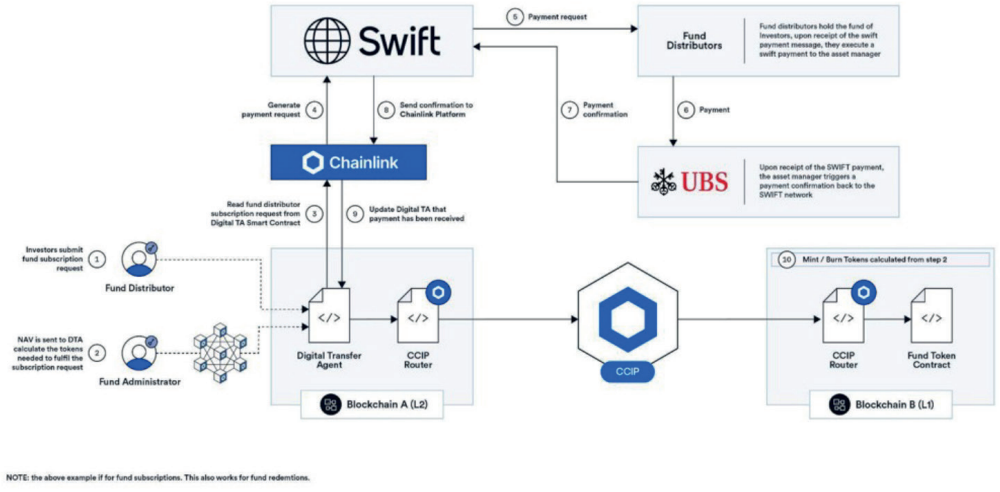
At the core of **Chainlink is the Chainlink Runtime Environment (CRE)**, a developer platform and decentralized execution environment for composing and orchestrating complex financial workflows across chains and offchain systems, addressing a key pain point of integrating existing systems with blockchains. Built upon CRE are open standards, each addressing a key dimension of end-to-end interoperability:

1. **Data standard** – Underpinned by the Onchain Data Protocol (ODP), the Chainlink data standard defines how offchain data is aggregated, verified, and published across any blockchain. By standardizing how data moves across chains and systems, ODP creates a shared information fabric for tokenized finance.
2. **Interoperability standard** – Powered by **Chainlink's Cross-Chain Interoperability Protocol (CCIP)**, the Chainlink interoperability standard enables seamless, secure transfer of data and value across both public and private blockchains. It also supports the **Cross-Chain Token (CCT) standard**, which makes any token natively transferable across chains without modifying its code.
3. **Compliance standard** – Based on the Onchain Compliance Protocol (OCP), the Chainlink compliance standard defines how identity, policy, and regulatory requirements are enforced in onchain workflows. Together with the **Chainlink Automated Compliance Engine (ACE)**, institutions can extend their existing compliance infrastructure onchain and ensure compliance rules and verified identities are portable across networks, preserving trust as assets move globally.
4. **Privacy standard** – The Chainlink privacy standard defines how sensitive data and value transfers can be executed without revealing confidential information, whether by encrypting cross-chain transactions, limiting onchain data exposure, or verifying offchain data privately.

Source for full image: https://blog.chain.link/wp-content/uploads/2025/10/Chainlink-Stack-Cropped-scaled.png

CRE unifies these standards on a single platform and makes them composable into complex workflows that interact across onchain and offchain systems. The result is a single, cohesive interoperability standard that can power the end-to-end lifecycle of tokenized asset transactions while meeting institutional-grade requirements for security, compliance, and reliability. This is how global finance will operate onchain.

One example of this approach is how a UBS tokenized fund used Chainlink to maintain its share registers and processes key fund lifecycle events across chains and existing systems, such as subscriptions/redemptions, settlement, and payments. The Chainlink data standard brought Net Asset Value (NAV) data onchain, CCIP enabled cross-chain Delivery vs. Payment settlement, and CRE connected existing offchain systems so asset managers can receive transaction updates and Swift messages to facilitate payments. Combined, these components unlock an end-to-end interoperability solution.



Source for full image: https://blog.chain.link/wp-content/uploads/2025/10/Swift-UBS-Case-Study-scaled.jpg

The Quiet Evolution of Global Finance: Tokenized Settlement and the Role of the CDM

TOKENOVATE

The evolution of financial instruments has always reflected a search for greater efficiency, security, and trust.

For centuries, ownership was represented by physical certificates, where possession conferred title and transfer occurred through delivery. This system worked when markets were small but became unmanageable as volumes grew and globalisation took hold. The shift to dematerialisation in the late twentieth century replaced paper with electronic records held in centralised registries, vastly improving speed and reliability but introducing new layers of intermediation and custodial fragmentation.

In effect, the operational risks of lost certificates were exchanged for systemic frictions in mobilising collateral and settling transactions across complex networks. The same challenge now confronts distributed ledger systems: rather than unifying markets, many have recreated the silos of the past.

The enduring lesson is that progress in finance lies not in form but in function.

What is Tokenization?

Tokenization is not a monolith. It does not describe a single technology or legal construct, but a spectrum of approaches that combine technical representation with legal effect. At its core, tokenisation is the act of representing an asset (whether a bond, share, or other instrument) as a digital token on a distributed ledger. That representation only has meaning if the token's technical structure aligns with the legal rights and obligations of the underlying asset.

From a legal perspective, tokens can take many forms: from cryptoassets, which exist entirely on-chain and outside formal legal systems, to security tokens, which exist on-chain but qualify as regulated financial instruments, to tokenized securities, which serve as digital twins of off-chain assets recorded elsewhere. Each form demands a distinct legal and data-modelling approach.

From a technological perspective, different distributed-ledger architectures can produce very different legal outcomes. Two systems may appear identical to a user yet diverge entirely in how they allocate ownership, enforce rights, or determine finality.

Tokenisation therefore sits at the intersection of technology, law, and market infrastructure. Small design choices in how a token functions can produce major consequences for how it is recognised in law and when, or whether, settlement is achieved.

The Role of CDM

These differences in legal, technological, and operational structures reveal a fundamental challenge. The tokenisation ecosystem today is balkanised. Each platform relies on its own identifiers, data models, and taxonomies. Integration is costly, and legal recognition remains uneven.

That is where the FINOS Common Domain Model (CDM) comes in. The CDM is not a new trading system or a rival blockchain. It is a set of open standards that describe what happens after a trade is made, how contracts are represented, how payments are calculated, how collateral moves, and increasingly, how tokenized assets operate.

Think of it as an Esperanto for financial data, a common language that allows machines, markets, and lawyers to understand one another.

Bridging Traditional and Digital Finance

The most immediate opportunity in tokenisation lies not in creating entirely new digital assets, but in transforming the vast universe of traditional securities that already underpin global markets. These instruments are governed by mature legal frameworks and trusted operational models, yet they remain constrained by legacy settlement systems that prevent true real-time transfer of ownership. Bringing such assets into a digital framework that preserves legal title while enabling T+0 settlement is the natural first step toward market modernisation.

Achieving this, however, exposes one of the hardest problems in tokenisation: keeping the digital and physical worlds in sync. When a share exists both in a traditional registry and as a token on a blockchain, which record represents the legal truth? Without alignment between the two, the "digital twin" model breaks down, eroding confidence and introducing additional risk into the system

The work I lead at the CDM Tokenized Assets Working Group is solving this precise challenge, bridging the divide between on-chain representations of value and the off-chain records that define legal ownership. Our approach uses the CDM to create a shared data and event framework that can describe both the on-chain and off-chain states, ensuring they remain synchronised throughout the trade lifecycle.

In practice, this means a token transfer can correspond directly to a recognised change in beneficial or legal ownership, recorded simultaneously across both systems. It allows programmable settlement to operate within the boundaries of established contractual and legal frameworks, ensuring that speed does not come at the expense of certainty.

Over time, the same framework can extend to natively digital assets, supporting a unified model for ownership and settlement regardless of where the record of title resides; whether with a custodian, a CSD, or a blockchain ledger itself.

This pathway shows that the CDM-based architecture is not a short-term bridge between analogue and digital systems, but a durable framework for the future, one that enables markets to evolve toward native digital issuance without sacrificing the legal certainty and operational integrity on which global securities markets depend.

The Future Is Interoperable

Tokenisation will not replace the financial system we have; it will connect it, making it more transparent, programmable, and efficient. But it can only do so if the legal, technological, and economic layers speak the same language.

That is what the CDM provides: a canonical data layer that bridges law, technology, and economics, enabling both the legal nature of digital assets and the mechanics of their transfer to be represented in a unified framework. It lays the foundation for the next generation of programmable, compliant financial infrastructure, one in which the line between on-chain and off-chain gradually disappears.

The transformation ahead will not come as a big bang. It will happen incrementally, as common standards replace fragmentation and bring coherence to the machinery of global finance. Tokenisation, properly standardised and modelled, is not a revolution apart from existing markets; it is the quiet evolution of the financial system itself.

Digital Asset Interoperability for Institutional Finance

WORMHOLE

Tokenisation has crossed the point of inevitability and increasingly embedded into real distribution.

The missing piece is not issuance capacity but market coherence. Assets, compliance controls, and liquidity venues live on fragmented ledgers with incompatible runtimes and inconsistent permissioning patterns. Fragmentation dilutes the properties that make institutional liquidity possible: singleness, consistency and predictable settlement.

Interoperability is becoming a balance sheet constraint and institutions need a layer that turns public and permissioned, EVM and non-EVM into one coherent settlement surface where regulated value can move with portable controls and auditable security assumptions. Wormhole's thesis is direct: interoperability for institutional finance must be messaging first, verifiable by default and designed to preserve asset integrity as distribution expands across heterogeneous environments.

When a tokenised treasury fund crosses a bridge and emerges as a wrapped derivative, it may carry a different regulatory classification, altered collateral eligibility and a new counterparty in the custody chain. A token moved, but the asset did not. This failure mode is why distribution has not produced liquidity escape velocity.

Institutional markets work because standards preserve singleness while enabling distribution. Tokenisation needs the same outcome across ledgers, one authoritative instrument identity and one control surface as execution venues proliferate.

Cross-runtime translation needs explicit verification

Interoperability is often described as connectivity. For institutions, it is translation across divergent computational models with different finality and execution constraints. EVM semantics are not Solana's runtime, Move chains enforce different invariants and permissioned environments introduce their own boundaries. Wormhole integrates at the level required to observe events, interpret state transitions with an extremely high degree of confidence and execute destination side settlement logic that respects each chain's constraints. Today, Wormhole integrates ten heterogenous runtime families and settled over one billion arbitrary messages over those venues.

Translation is where hidden risk accumulates. If an interoperability layer cannot produce a destination-verifiable statement of what happened on the source, the system devolves into operational trust and manual reconciliation and that is not scalable market infrastructure.

What institutional grade interoperability must guarantee

Institutional interoperability is not a bridge feature, it is a set of verifiable guarantees.

It preserves unified liquidity. Moving an asset across runtimes cannot create multiple non-fungible representations that require liquidity pools, wrappers or bespoke arbitrage paths to maintain price coherence.

It makes compliance portable. Platform level wallet whitelists put the record off-chain and create single points of failure. A stronger pattern uses programmable token standards with embedded identity and transfer logic so the asset enforces eligibility at transfer time across custodians, venues and chains. Standards such as ERC-3643 or zero-knowledge verification mechanisms present contract level checks that can encode KYC/AML status, jurisdictional constraints and other limits.

It supports external policy proofs. Many obligations cannot live purely onchain, so future proof architectures allow transfers to carry signed policy payloads that the destination verifies before finalisation, mirroring how CSDs validate settlement instructions before release.

It makes security assumptions explicit. Institutions govern trust thresholds, but only if the verification path is legible, auditable and monitorable.

Arbitrary messaging is the narrow waist

Wormhole is built around one institutional friendly abstraction: arbitrary, verifiable messages that carry standardised instructions across chains with token movement as an application. The core is message integrity and destination-side verification.

Wormhole's security model centres on a distributed Guardian Network of 19 independent, reputable, well-known entities that transparently observe source chain events and produce signed attestations. A message becomes actionable only after a supermajority threshold is met and destination contracts verify the signature set onchain before execution. This produces an auditable trust model where thresholds are explicit and assumptions can be evaluated in Byzantine fault tolerance terms rather than treated as an opaque relayer promise.

Wormhole supports native supply preserving transfer patterns and the operational controls production deployments required with its Native Token Transfers (NTT) including separation of incident-response authority from day to day administration, with rate limits that bound exposure during anomalies and arbitrary queueing. These controls matter because they translate interoperability from an engineering convenience into something operations and risk teams can run. Wormhole's NTT is the mature venue of choice for native assets such as SOL, AVAX, MON and M^0's M token, driving billions of dollars in onchain flows and providing standards-conformant issuance patterns that remain flexible. Issuers can deploy tokens to canonical interfaces with redemption guarantees while enabling cross-ledger distribution under explicit verification.

Institutional distribution at scale

This architecture is already being selected for regulated distribution.

Securitize chose Wormhole as its official interoperability provider for all current and future tokenised assets, and later announced Wormhole live as its primary interoperability solution.

BlackRock and Securitize expanded BUIDL across seven blockchains, a concrete signal that large scale fund distribution is being designed around verifiable multichain mobility rather than chain specific silos. BUIDL's assets under management amount to roughly $2.85B and its expansion to BNB Chain with Wormhole also coincides with its use in institutional collateral contexts. The market increasingly treats multichain portability as a functional property.

Centrifuge selected Wormhole as its multichain infrastructure partner starting with Anemoy's Janus Henderson Treasury Fund, Apollo's tokenised credit product ACRED has been rolled out across multiple public chains, and VanEck's VBILL treasury product follows the same pattern. This model extends today beyond treasuries into higher complexity private credit distribution.

Verification trajectory

Institutions will demand continuously tighter verification over time. Wormhole's verification model is built to evolve toward stronger cryptographic assurances as zero-knowledge proof systems mature and costs decline, while preserving a stable message and execution surface for issuers and applications. The key point is continuity, the system continues to raise assurance levels without forcing every issuer and venue to rebuild their distribution architecture.

Tokenisation's next phase will be decided by whether institutions can distribute regulated value across many environments while preserving singleness of supply, portable compliance and auditable security. Wormhole is engineered around the primitive that makes that possible: arbitrary messaging with explicit verification, paired with supply-preserving mobility patterns and operational controls that institutions can govern. The proof is no longer theoretical, institutional markets are selecting interoperable distribution as core infrastructure and they are doing it in a way that keeps the ass asset the asset.

From walled gardens to gateways: Legal and regulatory aspects of DLT interoperability

TRAVERS SMITH

Much of the focus on interoperability between distributed ledger technology systems often, for understandable reasons, concentrates on the technological aspects: how can two (or indeed more) separately developed protocols interact with each other in a fashion sufficiently seamless to be commercially useful?

For lawyers (the author practises in England and Wales), this question, while interesting, is merely one of a much wider set of questions. This article focusses briefly on introducing three aspects:

- Settlement finality
- Conflict of laws
- Legal and regulatory harmonisation

But first, while acknowledging the novelty and innovative nature of DLT, a brief history lesson.

The challenges of interoperability are not wholly new, and aspects of the three points set out above were the subject of intense scrutiny within the European Union at the beginning of the 21st century. In particular, the Giovannini Report, commissioned by the European Commission and published in 2001 (with something of a sequel in 2003), was a seminal review of barriers to efficient cross-border clearing and settlement within the EU. While focused on traditional (non-DLT) financial market infrastructures (FMIs), the insights from Professor Giovannini remain highly relevant when considering interoperability challenges for DLT-based systems. Fifteen barriers to cross-border clearing and settlement were identified, which – as readers will grasp – ranged across legal and technical issues, as well as national market practices.

The challenges of achieving DLT interoperability are similar, but on a potentially global scale, and with a wider range of use cases (Giovannini having been thinking predominantly about the securities markets), notably the use of stablecoins for settlement of the payments leg.

From a technological perspective, bridges (protocols that can be used to effect the ostensible passage of a token from one blockchain to another) are routinely cited as the solution. However (and depending on the design of both the relevant blockchains and the bridge), from a legal perspective, bridges can pose even more questions. For example, many bridges operate by locking the original token on the "origin" blockchain, and then minting a new token on the "destination" blockchain. This latter token may, in effect, be a "tokenised token" representing ownership of the original token. Under laws such as the EU's Markets in Crypto Assets Regulation (MiCA) the new token could have a different regulatory treatment to the old token. The question then arises: is that "interoperability", or merely a complex workaround?

Settlement finality

This is a legal concept, designed to protect the integrity and stability of systemically important FMIs, by restricting the scope for participants (or those acting on their behalf) to challenge or reverse transactions. For securities and cash, it has its own body of law. In the United Kingdom, the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 are derived originally from EU legislation, but are now open, in principle, to possible divergence and extension to other asset classes.

This legislation "switches off" general rules in insolvency law, and market participants and regulators rely on finality to assess risk, regulatory capital, insolvency implications, and systemic stability. The key questions in this regard include:

- **When is finality achieved?** In traditional centralised systems, finality is often defined by the rules of the relevant system or national law. With interoperable DLTs, each network may have distinct consensus mechanisms (most obviously proof-of-work versus proof-of-stake), different rules on reversibility, or even varying dispute resolution processes (or none).
- **Which system determines finality?** If a transaction transferring value or title traverses two or more ledgers, disagreement may arise as to which system's rules (and at which stage) should determine when the settlement is truly final.

The latter point brings us naturally to a discussion of conflict of laws.

Conflict of laws

It is perhaps trite to observe that DLT systems can be "everywhere and nowhere", but for lawyers this adds an additional edge to the question of which system's rules apply, because it may not even be certain which jurisdiction's laws apply in the first place.

Identifying the lex situs (location of the asset – potentially significant for certain legal purposes) is particularly problematic. Under English law, for many financial assets (including book-entry securities), the situs is often tied to the location of the register. But in DLT, registers are distributed, and where the governing law is unspecified, multiple conflicting laws might be asserted to determine an issue or dispute.

The market is therefore confronted with (at least) the following questions:

- Which law(s) govern(s) title transfer or the validity of settlement?
- Which courts have jurisdiction in case of a dispute or insolvency?

At the time of writing, the Law Commission (a government body charged with projects to reform the laws of England and Wales) is engaged in a project looking at the private international law treatment of digital assets. It currently proposes an approach under which English courts would develop a special body of law applying to digital assets issued on globally distributed systems. This has misleadingly been dubbed the "supranational" solution (misleading given that this would also require other jurisdictions independently to do the same, with no guarantees of harmonisation).

The author has serious reservations about this approach, far preferring a solution based on party autonomy (i.e. allowing the system or cryptoasset itself to specify its own governing law, which is in any event conceptually aligned with the idea of a consensus mechanism) with fallback options where there is no choice of law.

Discussing harmonisation is the logical next step.

Legal and regulatory harmonisation

While decentralisation maximalists may recoil at the concept, true interoperability at scale is highly likely to require some level of harmonisation and standardisation by central banks, legislators and regulators. Key extant global projects with this aim include work carried out by UNIDROIT and the Hague Conference on Private International Law; work is also being conducted by the Bank of International Settlements and IOSCO.

The Giovannini Reports reached the unavoidable conclusion that inter-operability needs some level of standardisation to be delivered effectively. Private sector initiatives can achieve a great deal in the context of a single system, but only so much on interoperability across borders and legal traditions.

It is up to lawyers to help the industry and policymakers strike the right balance: links, not cuffs.

Unlocking identity to enable digital asset scalability

Identity is a core pillar supporting a sound financial system.

Without trust, security and legal confidence in the counterparties to financial contracts, financial systems must fall back on informal sources of trust that undermine efficiency, access and the capacity of the financial system to perform its primary function of [AK1] capital allocation. Identities of counterparties – issuers, beneficiaries, intermediaries and investors must be verifiable, rooted in applicable national or cross-jurisdictional legislation. And crucially, identity solutions must be shared – in other words, stakeholders need to be able to ensure that references to a specific entity are commonly agreed upon.

Smart contracts and ledger-based infrastructure challenge how we deal with identity in the financial system. Licensed market participants act as trust anchors, ensuring compliance with regulatory requirements.. They use third parties to collect data about clients and counterparties from various sources, but ultimately all originate in roots managed or overseen by government authorities. Identity, especially for legal entities, is a public construct. Financial Market Infrastructures (FMIs) also validate participants and assign identifiers to create common references and safeguard integrity. Yet today, each market participant and FMI repeats the process of due diligence and identity verification, leading to inefficiencies and a proliferation of identifiers across systems. As infrastructures become more open and interconnected, this repetition hampers efficiency and interoperability.

Decentralized financial (DeFI) ecosystems aim to enhance access and lower transaction costs without sacrificing trust and control. Today though, we face a situation in which digital asset markets are simultaneously fragmented and concentrated while also suffering from gaps in trust and integrity. Parties controlling addresses on ledgers are not published; issuers of assets are difficult to verify; compliance with AML requirements remains costly and cumbersome. These gaps undermine the other benefits of DeFi architectures and even basic financial instruments. They also undermine the potential of smart contracts that are designed to automate more complex, multi-party interactions between financial and Real-World Assets (RWA) and events.

GLEIF and the vLEI – a brief introduction

The Legal Entity Identifier (LEI) was created in the wake of the 2008 financial crisis as a global standard for identifying legal entities in financial transactions. Each LEI is a unique 20-digit alphanumeric code tied to key reference data about the entity. This reference data is validated and standardized according to rigorous quality controls and in accordance with the ISO 17442 standard. The LEI data includes Level 1 "Who is who" information – the entity's official name, registered address, country of

incorporation, registration number, etc. – and Level 2 "who owns whom" information – the entity's parent/children relationship. Each LEI record carries metadata such as the date of last update, the verification status of the data and the entity's status (e.g. active, merged, expired).

The verifiable LEI (vLEI) is a high assurance digital credential that can be used verify counterparties across digital as well as legacy infrastructure. The vLEI binds the identity of a (i) legal entity with (ii) a legal representative of it and (iii) their specific role within a high assurance, highly secure Identifier. The vLEI is issued by Qualified vLEI Issuers (QVI) that adhere to the vLEI Ecosystem Governance Framework (EGF), ultimately overseen by the Regulatory Oversight Committee (ROC). vLEI credentials build explicitly on a chain of trust consistent with the Trust over IP Foundation model.

The vLEI is designed for a world of decentralized verifiable smart contracts and machine-readable processing. It uses Autonomic Identifiers (AID) that enable the controller's identity to be verified via a network of decentralized 'witness servers'. Yet the LEI embedded within it - and adherence to the EGF -ensures that, unlike other Decentralized Identifiers (DIDs), ownership can be traced back to an original root of trust anchored in the Global LEI System and its oversight by the ROC. The result is a hybrid between a federated and a decentralized system, providing high trust and interoperability within a scalable global network. Trust in the vLEI links back ultimately to local registries through the LEI and a network of Accredited LEI issuers. But it operates as a decentralized network because any entity can obtain a vLEI without intervention from their local registry and anyone can access witness networks to verify the owner/controller of the AID and vLEI Credential.

Addressing identity in digital asset markets

Digital Asset ecosystems and Smart Contracts have several roles in which identity and identifiers need to be adapted. There are also several market structures to consider as digital identity solutions are developed.

Different market approaches exist to identify controllers of addresses on-chain or holding off-chain roles.

1. Decentralized with federated intermediary controlled identity

Native identifiers on chain can be KYC'd by intermediaries in accordance with any local rules. The ledger or oracle intermediaries providing access are responsible for the assurance of identity and compliance.

2. Intermediary controlled identifiers mapped to unique identifiers

Oracles link their customer identifiers and files to an identifier issued independently of any specific chain and provide the trusted link to on-chain or smart contract transactions

3. Globally interoperable identifiers embedded in native applications

Whenever there is a need for an entity (or someone on its behalf) to prove who they are online, a vLEI can serve that purpose: Key Identity roles on chain and in smart contract ecosystems include (but are not limited to):

- **Digital onboarding and account opening:** The client representative uses a vLEI credential to prove their identity as an Issuer or to log into the onboarding portal of an infrastructure. The system automatically recognizes the person and their organization, eliminating the need for

separate identity uploads. The act of presenting the vLEI can even serve as the "e-signature" for forms, since it's a cryptographically signed proof of identity and intent.

- **Contract signing and consent:** Parties can use vLEI credentials to sign actions on the chain or a smart contract to verifiably demonstrate control. For example, when the CFO of a company signs a subscription agreement using her vLEI, the counterparty can immediately verify not only the signature's integrity but also that the signer was, at the time of signing, the CFO of the company with a valid LEI.
- **System-to-system authentication:** In securities services, clients often connect their internal systems to a custodian's or broker's systems via APIs or secure networks. vLEIs can be used to authenticate these connections. An API client can present a vLEI credential as part of its handshake, effectively saying "this API request is being made by a software agent of XYZ Corp.".
- **AI or automated agent representation:** Looking ahead, as artificial intelligence agents and bots take on roles in trading or client service, vLEIs provide a means for these non-human actors to carry an identity token of the organization they represent. For example, if an AI-based trading algorithm is negotiating trades on behalf of a fund, it could authenticate each message with a vLEI credential proving it is an authorized agent of that fund. This assures counterparties that they are dealing with a legitimate representative, not an impostor

Conclusion: issues to address, decisions to make

Smart contract standards will require highly secure, interoperable and automated ways to verify counterparty identity and control. Investors and intermediaries need to be able to trust and verify the status of issuers and asset holders; regulators will increasingly expect more robust compliance with AML, sanctions and cross-border controls; and smart contracts with more sophisticated structures will need to automate verification of other market participants, assets or events. The vLEI ecosystem can help financial markets in digital assets address these gaps through solutions that provide high assurance and already are designed to work across technology, markets and jurisdictions. As of September 2025, the vLEI ecosystem is still in evolution, with a limited number of QVIs. Early-stage engagement by GLEIF and its ecosystems participants within the smart contract working group can help to solve for a crucial element of future financial market infrastructures for digital assets.

[AK1] Intermediation is the current mechanism, not the primary function of financial systems. Blockchain aims at reducing (if not eliminating) unnecessary intermediation as much as possible so I would like to avoid using that term as to not look as we are preserving the current model which will evolve. Issuers are not intermediaries, beneficiaries neither. They are at the only parties that maters, ultimately.

Section 4

Quotes from the SODA community

Quotes from the SODA community

ADIA ⁞ Lab

> When a financial institution approaches Distributed Ledger Technology, selecting the appropriate infrastructure can be the first challenge. Both private, permissioned distributed ledgers, that were often the first choice of regulated entities, and later public blockchains, are often siloed ecosystems that connect to different DLT solutions.
>
> This largely explains the slow and cautious entry of regulated institutions into the tokenization space. For highly regulated and risk-sensitive entities such as sovereign wealth funds, the absence of secure and standardized interoperability across distributed ledgers has been a decisive obstacle. Institutions focus on regulated financial instruments, whose tokenized versions require strong assurances of rapid convertibility into the underlying reserves or into a liquid reference currency, particularly for their use as collateral or settlement instruments. In practice, this means that a tokenized asset must be able to move seamlessly and be redeemed quickly, regardless of which distributed ledger it was issued on or currently resides on.
>
> The need for cross-chain liquidity and operational neutrality is particularly strong in jurisdictions such as the United Arab Emirates (UAE), with advanced regulatory frameworks for virtual assets, most notably stable coins, and progressing toward a central bank digital currency. The existence of a regulated digital cash leg on distributed ledgers is a push towards standardization and interoperability, that needs to extend to all tokenized assets, to allow eventually the transferability and convertibility guarantees that financial institutions demand.
>
> Ultimately, the success of tokenization in the regulated space depends on the establishment of standards capable of bridging different distributed ledgers, traditional and digital finance, and both private and public infrastructures. This can provide the strongest guarantee that digital assets maintain liquidity, legal certainty, and trustworthiness across the global financial system.

ADIA Lab

Stellar

> At the Stellar Development Foundation, we believe that the future of digital finance depends on standards – not just for technology, but for trust. Establishing clear, open frameworks for tokenizing real-world assets is essential to ensuring that every digital representation of value carries the transparency, compliance, and verifiability required to operate at scale. When assets are tokenized using shared standards, they become more than digital replicas – they become programmable, interoperable instruments capable of moving securely and efficiently across global markets.
>
> Interoperability is the force multiplier that brings this vision to life. By connecting diverse blockchains, financial institutions, and payment infrastructures,

interoperability transforms isolated digital asset ecosystems into a unified network of value exchange. This is why, at SDF, our work goes beyond supporting token issuance on the Stellar network – we actively promote open token standards, develop tools that make compliance seamless, and collaborate across industries to align technology with real-world regulation and financial access.

From powering tokenization use cases that bring tangible assets like cash, commodities, and credit into the digital economy, to fostering cross-chain solutions that eliminate friction, our mission remains clear: to build a future where every asset, on every network, can move with the same ease, transparency, and inclusivity as information does today.”

Stellar Development Foundation

ICMA

“The evolution of digital asset markets depends not just on technological innovation, but on the standards that make that innovation meaningful. Through the Bond Data Taxonomy, ICMA has defined a technology agnostic data model for securities, ensuring that every tokenised instrument – whether on a blockchain, traditional registry, or hybrid system – carries the same core attributes of trust, governance, and transparency.

Standards create the common language that allows disparate systems to connect, collaborate, and interoperate seamlessly. When assets are defined consistently and interpreted uniformly, networks can exchange value with confidence, efficiency, and integrity. In this way, standards are not just rules – they are the foundation for a truly interoperable, resilient, and inclusive digital capital market of the future.”

International Capital Market Association (ICMA)

Libeara

“With well over US$30 billion tokenized assets on-chain today, the industry has come a long way. But what we have ended up with is a landscape of impressive yet siloed Proofs-of-Concepts (PoCs) that are struggling to scale into a cohesive, liquid market.

Our future will be a “network of networks”, where tokenized assets move seamlessly between permissioned and/or public ledgers, and whose value is universally recognized across the digital asset realm. What we have to work towards is more than just a technical bridge, it is network fungibility—where a tokenized BlackRock fund on one network is treated as legally and functionally identical to the same fund on another network. This requires a new layer of shared standards, identity frameworks, and legal agreements.

The responsibility of the early market participants, many of whom have contributed to this whitepaper, is to build this infrastructure right,

and that means making sure that universal baseline standards are established at the industry level. Only then can we achieve a unified market infrastructure where tokenized assets are issued, traded, and settled with the same finality and security as traditional securities today.

Libeara

Canton

"The future of global finance will not be built on islands. It will run on networks that can trust and transact across boundaries, without compromising on threshold regulatory issues like privacy. At Digital Asset, we see interoperability as foundational to unlocking the composability and velocity of blockchain at scale.

Beyond the technical need for composability at the smart contract level, standards for onchain real-world assets, and open network principles make this future possible. Canton's CIP-56 gives on-chain securities a common language so assets, cash, and workflows compose safely with atomic settlement and privacy by design. Today, that standard underpins a network of independent networks that already includes over $6T in real-world assets and $281B+ in average daily on-chain repo activity, evidence that this isn't theory.

In addition, an open network, with independent governance by The Canton Foundation, means firms focused on multi-chain interoperability, such as Ownera, Wormhole, Chainlink and LayerZero build with Canton too. This extends that same standard across networks in a controlled and consistent way. Our goal is a connected financial system where trust is programmable, privacy is preserved, and institutions can innovate without giving up control."

Canton Network

SOLANA FOUNDATION r3.

"The next chapter of digital finance will be defined not by isolated innovation, but by connected trust. As trillions of dollars in real-world assets transition on-chain, standards for tokenization are the cornerstone that ensures every digital asset is created, governed, and exchanged with transparency, auditability, and regulatory confidence. Without shared frameworks, tokenized assets remain confined within silos; with them, they become the foundation of a new, interoperable financial fabric.

Interoperability is the catalyst that transforms these standards into global infrastructure. When tokenized assets can move securely across institutions, networks, and jurisdictions, they cease to be experiments and become instruments of real-world value. This requires performance, compliance, and resilience – the precise intersection where Solana and R3 meet.

The R3-Solana partnership brings together two complementary strengths: Solana's high-throughput, energy-efficient public blockchain and R3's proven infrastructure for regulated markets. Together, we are building the connective tissue between public-chain innovation and institutional trust – enabling assets, liquidity, and participants to flow freely while maintaining the privacy and governance demanded by global finance.

The future of tokenized assets depends on this convergence: open standards, interoperable systems, and shared trust between institutions and technologies. That is the vision driving our collaboration – a unified ecosystem where performance meets compliance, and digital assets move as confidently as the markets they represent.

Solana Foundation & R3

ARCHAX

Archax firmly believes that the future of all traditional financial markets is on-chain and this digitally-native world is fast becoming a reality. One only has to look at the increasing momentum around real-world asset (RWA) tokenization to see evidence of this. The days of 'test-cases', 'pilots' and 'proof of concepts' are over, and we are now seeing production projects that tokenize RWAs and then use those tokens in innovative ways – with collateral mobility being a good example of this.

With our institutional partners and clients, such as Aberdeen, Blackrock, Federated Hermes, Fidelity, Legal & General, Lloyds Bank and State Street, we are proud be one of the key regulated digital asset platforms at the forefront of this digital revolution. The days of 'dumb assets' sitting on balance sheets are over, as, through tokenization, these assets can now get 'smart' and be used in all sorts of new and interesting ways.

But for all this to go mainstream and for institutional adoption to scale, interoperability and standards are key. We need to get to the point where we stop talking about the technology and it gets taken for granted instead. As such, we are proud to be contributing to this important MIT-SODA initiative.

Archax

Veridian by Cardano Foundation

Advancing decentralized public infrastructure has been at the forefront of the Cardano Foundation's mission. We recognize the indispensable role of open standards and comprehensive protocols in establishing cohesive and compliant ecosystems. The Foundation's development of Veridian exemplifies this commitment, providing a truly agnostic identity solution engineered for integration with financial institutions, enterprise entities, and sovereign states.

At the Cardano Foundation, we deem it essential that the forthcoming generation of on-chain digital assets supports the integration of existing governance frameworks, regulatory requirements, and established roots-of-trust. The foundational elements for a compliant and future-proof decentralized financial infrastructure are now emerging. However, the subsequent trajectory toward an interconnected, efficient, and compliant digital marketplace necessitates a unified approach—one that prioritizes protocols over platforms, interoperability over siloed interests, and mandates the highest levels of assurance by default.

Veridian by Cardano Foundation

Every interoperability challenge in this paper ultimately traces to one foundational gap: identity. Cross-chain bridges cannot verify counterparties. Data standards cannot automate compliance checks. Smart contracts cannot distinguish legitimate issuers from those attempting to tokenize assets fraudulently. Without on-chain identity, even perfectly interoperable technical infrastructure forces RWA tokens onto centralized exchanges, undermining the core vision of open, liquid markets.

Current identity solutions perpetuate this failure through architectural compromises. Centralized verification concentrates credentials into honeypots vulnerable to catastrophic breach. Platform-controlled whitelists create vendor lock-in. Private/permissioned networks achieve compliance by eliminating the open liquidity that makes interoperability valuable. These trade-offs explain why institutional adoption remains constrained.

The I-SODA initiative offers a historic opportunity: establishing global interoperability standards that incorporate robust identity from the foundation rather than as an afterthought. The vLEI ecosystem, combining G20-endorsed Legal Entity Identifiers with KERI's decentralized infrastructure, provides what these standards require. KERI enables verifiable smart contracts with quantum-resistant security and compromise recovery while each participant operates sovereign infrastructure.

By embedding vLEI-based identity verification within I-SODA's framework, the ecosystem can bridge regulatory legitimacy with cryptographic trust, transforming tokenization from fragmented experiments into genuinely interoperable global markets.

Identity is not peripheral to interoperability standards. It is foundational.

Key State Capital

GFT udpn Universal Digital Payments Network

UDPN sees interoperability as the cornerstone of a truly global digital financial system. The MIT-SODA white paper highlights the urgent need for standardized tokenization workflows that transcend technological silos. As digital currencies and tokenized assets proliferate, the ability to transact across networks—securely, compliantly, and instantly – becomes essential. UDPN's mission aligns with this vision: enabling regulated digital payments and asset transfers across diverse platforms. We support the creation of MIT-SODA and its commitment to open standards, legal clarity, and technical neutrality. This initiative lays the groundwork for a future where digital assets and payments are universally accessible, programmable, and trusted – empowering institutions to innovate without compromising compliance or control.

GFT UDPN

XRP LEDGER

> The next chapter of digital finance will be defined by networks that can interoperate with trust, compliance, and scale. As real-world assets move onchain, interoperability standards are essential to ensure that tokenized value remains transparent, auditable, and governed across jurisdictions. Without shared frameworks, liquidity is constrained; with them, digital assets become the foundation of a truly connected financial system.
>
> Interoperability is what transforms these standards into operational infrastructure. The XRP Ledger, with XRP as its native asset, is designed as a foundational platform for institutional finance, bridging traditional finance with the digital economy through efficient, regulated, and high-integrity settlement across core use cases like cross-border payments, tokenization, and liquidity management. Our goal is to support an open, interoperable ecosystem where value can move securely and compliantly without friction across networks.

XRP Ledger Foundation

Interledger FOUNDATION

> If we want digital finance to actually work for people, not just the folks already inside the system, interoperability has to be the starting point. Without open standards, tokenized assets end up stuck in little islands that don't talk to each other. That might make things slightly more efficient for incumbents, but it does nothing for those usually left out.
>
> When we agree on shared frameworks, a common way to describe an asset, consistent functions to move it, and legal rules that don't fall apart when you cross a border, value can flow with the same ease as data packets hopping across networks. Fees drop, settlement times shrink, products once out of reach become accessible. The shipping container unlocked global trade because everyone agreed on how it should work. Open rails, not walled gardens, that's how we build finance that actually includes everyone.

Interledger Foundation

Section 5

The scope of the organization

Regulated finance; real world assets only

I-SODA will only focus on regulated financial instruments; real world assets that are currently traded within the parameters of regulated finance. Some blockchains also host many other tokenized forms of value including memecoins, NFTs, voluntary market carbon credits and crypto-native governance tokens, and these will not be covered by this work.

The payment leg: ISO 20022, cash on-chain, stablecoins, tokenized deposits and CBDCs

Every asset bought (regardless of whether it is tokenized or not) needs to be paid for, and all observers are united in the view that there has to be an effective on-chain payment solution; such as a stablecoin or something similar. Without such functionality the 'token-based habitat' will remain out of reach, even if, in the short term, some tokenization projects are using traditional rails for the 'cash leg'. As such, the organization regards backed stablecoins, and other forms of cash-on-chain, as an essential component of our activity and they will be included as the members of the organization demand. More far-reaching on-chain public money solutions, such CBDCs, are not a part of I-SODA's work today.

Next steps and timelines

Join I-SODA

The Interoperability Standards organization for Digital Assets (I-SODA) is open to all participants working in regulated finance and digital assets. Following the IETF model the organization will create a 'leadership board' of systemically important financial institutions (FMIs) and large technology actors in the blockchain space.

If your institution wants to join I-SODA at MIT please get in touch

Develop and publish token standards for a specific use case

MIT and SODA Services team of experts are currently working on open standards for tokenization use cases in regulated finance. We work with financial institutions, token solution providers and FMIs as they create the tokenization workflow.

Please get in touch to learn more about our standards development work

Industry Survey

SODA is be conducting an industry survey to measure the business impact of tokenization on investment banks.

Please get in touch if you wish to participate

MIT Connection Science
the technology of innovation

MIT Connection Science

MIT Connection Science is a world-wide alliance of progressive companies, nations, and multilateral organizations seeking to understand how to create data, analytical, and digital network systems that can improve the world.

About SODA Services Ltd

SODA Services Ltd. is a digital money and digital assets consultancy business based in London. SODA Services works with technology providers, public sector institutions, international organizations delivering token solutions, research and advisory services in multiple countries.