

JUNE 2025

vLEI on-chain:
Verifiable Smart Contracts



KEY STATE CAPITAL

 Cardano
Foundation



vLEI on-chain:

Verifiable Smart Contracts

© 2025 Key State Capital, Cardano Foundation, and Global Legal Entity Identifier Foundation (GLEIF)

This report, “vLEI on-chain: Verifiable Smart Contracts”, was jointly authored by Key State Capital, the Cardano Foundation, and the Global Legal Entity Identifier Foundation (GLEIF), and was published in June 2025.

This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/). You are free to share and adapt the material, provided appropriate credit is given to all three contributing organizations.

Table of contents

01	Abbreviations	4
02	About	5
	2.1 About the publishing organizations	6
03	The Problem: Smart Contracts Current Limitations	7
	3.1 The Identity Crisis: No Connection to Real-World Entities	8
	3.2 The Inevitable Reality: All Keys Get Compromised	8
	3.3 Systemic Security Vulnerabilities	9
	3.4 Lack of on-chain Identity creates Broader Systemic Risks	9
	3.5 Consequences	9
04	The Breakthrough: vLEI & KERI	10
	4.1 The vLEI	11
	4.2. Intro to KERI: the foundation of vLEI	13
05	Overcoming the Limitations with Verifiable Smart Contracts	14
	How Verifiable Smart Contracts become real: A technical roadmap	15
	5.1 Address Attribution: The end of whitelists	16
	5.2. De-Fi Fraud prevention	20
	5.3. Compromise Recovery	24
	5.4. Compliance: Travel Rule Protocol example	28
	5.5 Smart Contract Evolution	32
06	Which building blocks and infrastructure are needed?	33
	6.1 More Issuance and Infrastructure	34
	6.2. Consensus on Standards and Implementation	35
	6.3. Global KERI Infrastructure: Watchers and Oracles	35
	6.4 The Race for Global Infrastructure	38
	6.5 Conclusion	38
07	Why now: The Regulatory Imperative and Market Transformation	39
	7.1 The Knowledge Gap Creates Opportunity	40
	7.2 Regulatory Momentum is Accelerating	40
	7.3 The Paradigm Shift is Inevitable	40
	7.4 A Call to Action	40
08	Conclusion	41
09	Sources	42

01. Abbreviations

ACDC	Authentic Chained Data Containers	LEI	Legal Entity Identifier
AI	Artificial Intelligence	LOU	Local Operating Units
AID	Autonomic Identifier	MiFID II	(European) Markets in Financial Instruments Directive 2014
API	Application Programming Interface	MiFIR	(European) Markets in Financial Instruments Regulation
AWS	Amazon Web Services	OOR	Official Organization Role
BIS	Bank of International Settlements	OTC	Over the Counter
CEO	Chief Executive Officer	PKI	Public Key Infrastructure
CTO	Chief Technology Officer	QVI	Qualified vLEI Issuer
DAO	Decentralized Autonomous Organization	ROC	Regulatory Oversight Committee
DAI	DAI Stablecoin	RWA	Real-World Assets
DeFi	Decentralized Finance	S3	Simple Storage Service (Amazon's cloud storage)
DEX	Decentralized Exchange	SME	Small-to-Medium Enterprise
DID	Decentralized Identifier	SOX	Sarbanes-Oxley Act
EBA	European Banking Authority	TLS	Transport Layer Security
ECR	Engagement Context Role	ToIP	Trust over IP Foundation
ESMA	European Securities and Market Authority	TRP	Travel Rule Protocol
EVM	Ethereum Virtual Machine	UI	User Interface
FATF	Financial Action Task Force	USDC	USD Coin
FDTA	(US) Financial Data Transparency Act	USDT	Tether USD
FSB	Financial Stability Board	UTI	Universal Transaction Identifier
G20	Group of Twenty	UX	User Experience
GLEIF	Global Legal Entity Identifier Foundation	VAT	Value Added Tax
IVMS	InterVASP Messaging Standard	VASP	Virtual Asset Service Provider
ISO	International Standards Association	vLEI	Verifiable Legal Entity Identifier
KEL	Key Event Log	KYC	Know Your Customer
KERI	Key Event Receipt Infrastructure	KYB	Know Your Business
MiCA	Markets in Crypto-Assets		

02. About

Smart contracts fundamentally lack verifiable identity. This creates a critical gap between on-chain activity and real-world entities. Current web3 oracle solutions have evolved to be great at transporting data, **but are not yet able to transport trust**. This missing trust layer prevents automated compliance, limits regulated use cases like RWA (Real-World Asset) tokenization, and ultimately blocks the seamless integration of traditional and decentralized financial systems. Additionally, the absence of robust identity verification and authorization mechanisms has left smart contracts vulnerable to sophisticated attacks, creating billions in damages annually.

The next generation of Smart Contracts: *Verifiable Smart Contracts*

A breakthrough in decentralized key management (KERI), now enables the creation of cryptographic identifiers with previously impossible attributes.

Key Event Receipt Infrastructure (KERI) is already being utilized outside of web3 by GLEIF (Global Legal Entity Identifier Foundation). **GLEIF is the issuer of the only globally adopted and mandated G20-initiated Legal entity Identifier, the LEI**, to issue the LEIs digitally verifiable counterpart: vLEI (verifiable LEI).

As vLEI adoption in the web3 ecosystem ramps up, the features which KERI's autonomic identifiers (AIDs), and therefore vLEIs, employ, will become available to smart contracts.

This upcoming leap in smart contract utility will be of a magnitude and scope which warrants the coining of a new term, **because vLEI-enabled smart contracts will enjoy capabilities & security which fundamentally differentiate them from regular smart contracts**.

This report coins the term Verifiable Smart Contract

A Verifiable Smart Contract is a smart contract that includes vLEI derived cryptographically verifiable information about the legal entity(ies) responsible for its creation or issuance, and its auditing where relevant, enabling automated regulatory compliance, enhanced fraud prevention, and compromise recovery and prevention mechanisms.

For highly regulated institutions, we predict that in the medium term, **the use of non-vLEI-enabled smart contracts will become unacceptable from a regulatory standpoint and in the long term from the retail perspective**.

This report examines the existing technological and regulatory developments that make this leap possible, analyzes the long-term ramifications, and explores the transformative impact on both the global web3 ecosystem and traditional financial sector. We also investigate how vLEI will enable the convergence of these two worlds and identify the missing infrastructure pieces needed to realize this vision.

While this report uses financial use cases such as tokenized shares and securities as examples, the described capabilities apply to all types of smart contracts including all imaginable types of RWA tokens such as property, real estate and trade receivables

2.1 About the publishing organizations



About Key State Capital

KEY STATE CAPITAL is a network of business angels conducting investment & advisory focused on empowering decentralized economies with verifiable data. We invest in early stage startups in the digital identity space and provide our portfolio companies with unparalleled reach, support, and guidance enabling them to scale internationally.

keystate.capital



About Cardano Foundation

The Cardano Foundation helps to nurture the present and future generations of developers in the Cardano ecosystem by building fast, secure, and cost-efficient solutions using a variety of coding languages that make onboarding onto Cardano easy.

cardanofoundation.org



About Global Legal Entity Identifier Foundation (GLEIF)

GLEIF manages a network of partners, the LEI issuing organizations, to provide trusted services and open, reliable data for unique legal entity identification worldwide. GLEIF services ensure the operational integrity of the Global LEI System. GLEIF is a globally active not-for-profit organisation and was created by the G20 in the wake of the 2008 financial crisis to bridge the gap between business registries.

gleif.org

03.

The Problem:

Smart Contracts

Current Limitations

Smart contracts—self-executing agreements with terms directly encoded in code—have revolutionized blockchain functionality, but operate with fundamental security vulnerabilities that have resulted in billions of dollars in losses. While substantial progress has been made in solving the “oracle problem” through various data providers and verification mechanisms, **a critical missing link remains: verifiable identity.**



3.1 The Identity Crisis: No Connection to Real-World Entities

Smart contracts have no native mechanism to verify who created them or associate them with specific real-world entities. This absence stems from a more fundamental problem—the lack of proper digital identity solutions in traditional systems that could be bridged to blockchain environments. While contract addresses are traceable, they provide no cryptographic assurance about the actual legal entities or individuals behind them. Organizations cannot make cryptographic assertions on-chain that are cryptographically tied to their verified identity.

This identity gap has become a critical regulatory concern.

The International Organization of Securities Commissions (IOSCO) explicitly addresses this challenge in their 2023 DeFi policy recommendations, stating that regulators should “*identify the persons and entities of a purported DeFi arrangement that could be subject to its applicable regulatory framework*,” particularly those “*exercising control or sufficient influence*” over DeFi financial products and services. The current inability to cryptographically link on-chain activities to verified legal entities directly impedes regulators’ ability to implement this fundamental oversight requirement.^[29]

3.2 The Inevitable Reality: All Keys Get Compromised

In blockchain systems, the security assumption that private keys can remain secure indefinitely is fundamentally flawed.

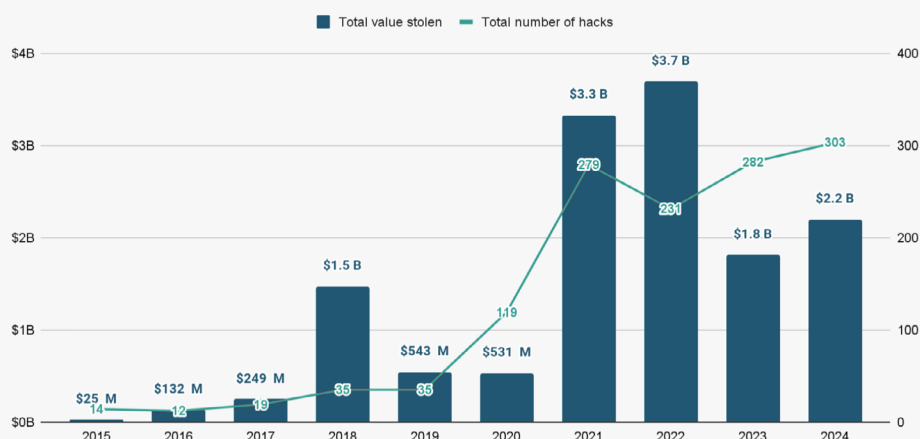
On a long enough timeline, all actively used cryptographic keys will eventually be compromised through various attack vectors including phishing, malware, insider threats, or sophisticated state-level attacks.

3.2.1 Catastrophic Real-World Failures

Recent major cryptocurrency hacks demonstrate these exact failure scenarios, resulting in billions in losses^[1]:

- ◆ **Bybit (February 2025): \$1.5 billion stolen** when attackers compromised Safe{Wallet} infrastructure through a supply chain attack. A single developer’s compromised laptop gave attackers access to AWS S3 credentials, allowing them to inject malicious JavaScript that deceived multi-sig signers into approving a delegate call transaction that transferred ownership to an attacker-controlled contract.^[2]
- ◆ **WazirX (July 2024): \$235 million lost** when attackers used interface spoofing to manipulate multi-signature wallet verification. Signers believed they were approving legitimate transactions while actually authorizing malicious contract upgrades.^[3]
- ◆ **Ronin Bridge (March 2022): \$625 million stolen** when attackers compromised 5 out of 9 validator keys through social engineering. Four validators were controlled by Sky Mavis, and a fifth was accessible through an improperly revoked whitelist permission from Axie DAO.^[4]
- ◆ **Radiant Capital (October 2024): \$58 million lost** through coordinated attacks on multiple signers using sophisticated malware that altered transaction data while displaying legitimate information to hardware wallet users.^[5]

**Yearly Total Value in Stolen in High-Profile Crypto Hacks
2015 - 2024**



Source: *The Chainalysis 2025 Crypto Crime Report*^[30]

3.3 Systemic Security Vulnerabilities

3.3.1 Critical Failure Points in Current Architecture:

- ♦ **Coordinated Phishing Attacks:** Attackers target multiple signers simultaneously using sophisticated social engineering
- ♦ **Insider Threats:** Malicious signers collude or are coerced, as seen in centralized validator setups
- ♦ **Infrastructure Compromise:** Shared infrastructure (like hardware wallet vendors, UI providers, or cross chain bridges) becomes a single point of failure
- ♦ **Supply Chain Attacks:** Compromise of development tools, UI frameworks, or signing interfaces affects all users

3.3.2 The Permanent Loss Problem

Once the threshold is breached, attackers gain complete control over the smart contract, and legitimate signers lose all access **permanently**. Even if some legitimate signers could prove their identity, the system remains untrustworthy because the compromised keys could still be used maliciously.

3.4 Lack of on-chain Identity creates Broader Systemic Risks

3.4.1 Regulatory Compliance Impossibilities:

Real-world assets (RWAs) tokenization is severely **limited**—forcing these assets to trade primarily on centralized exchanges because decentralized exchanges (DEXes) cannot guarantee regulatory compliance on-chain.

Without verifiable identity, automated compliance checks become impossible on-chain:

- ♦ Counterparty verification remains manual and error-prone
- ♦ Accountability is pushed off-chain, creating regulatory enforcement gaps

3.4.2 Fraud and Trust Issues:

- ♦ **Weak Provenance Assurance:** Cannot cryptographically verify who actually issued a contract/token, enabling impersonation attacks
- ♦ **Ineffective Whitelisting:** Current whitelisting relies on addresses rather than verified entities, creating administrative burden and security gaps
- ♦ **Limited Fraud Prevention:** Difficulty validating counterparties enables various financial frauds, particularly in DeFi
- ♦ **Oracle Trust Issues:** Oracles inject external data with limited accountability or verification of the source

3.4.3 Operational and Governance Limitations:

- ♦ **Cross-Chain Identity Fragmentation:** Identity and verification don't transfer reliably across blockchains
- ♦ **Absent Trust Transfer Mechanisms:** Without the ability to validate ambient keystate, trustless ownership delegation/transfer is impossible
- ♦ **Wildcat Distributed Governance:** DAOs and on-chain governance lack coordination & verification of participant legal status
- ♦ **Legal Enforcement Barriers:** Difficulty connecting on-chain activities to verified legal entities complicates regulatory enforcement

3.5 Consequences

These fundamental limitations have:

- ♦ **Constrained blockchain adoption in regulated industries** for over a decade
- ♦ **Created vulnerabilities that undermine the reliability of decentralized systems**, particularly when interfacing with traditional finance or legal frameworks
- ♦ **Resulted in billions of dollars in permanent losses** with no recovery mechanisms
- ♦ **Prevented the seamless integration of traditional and decentralized financial systems**

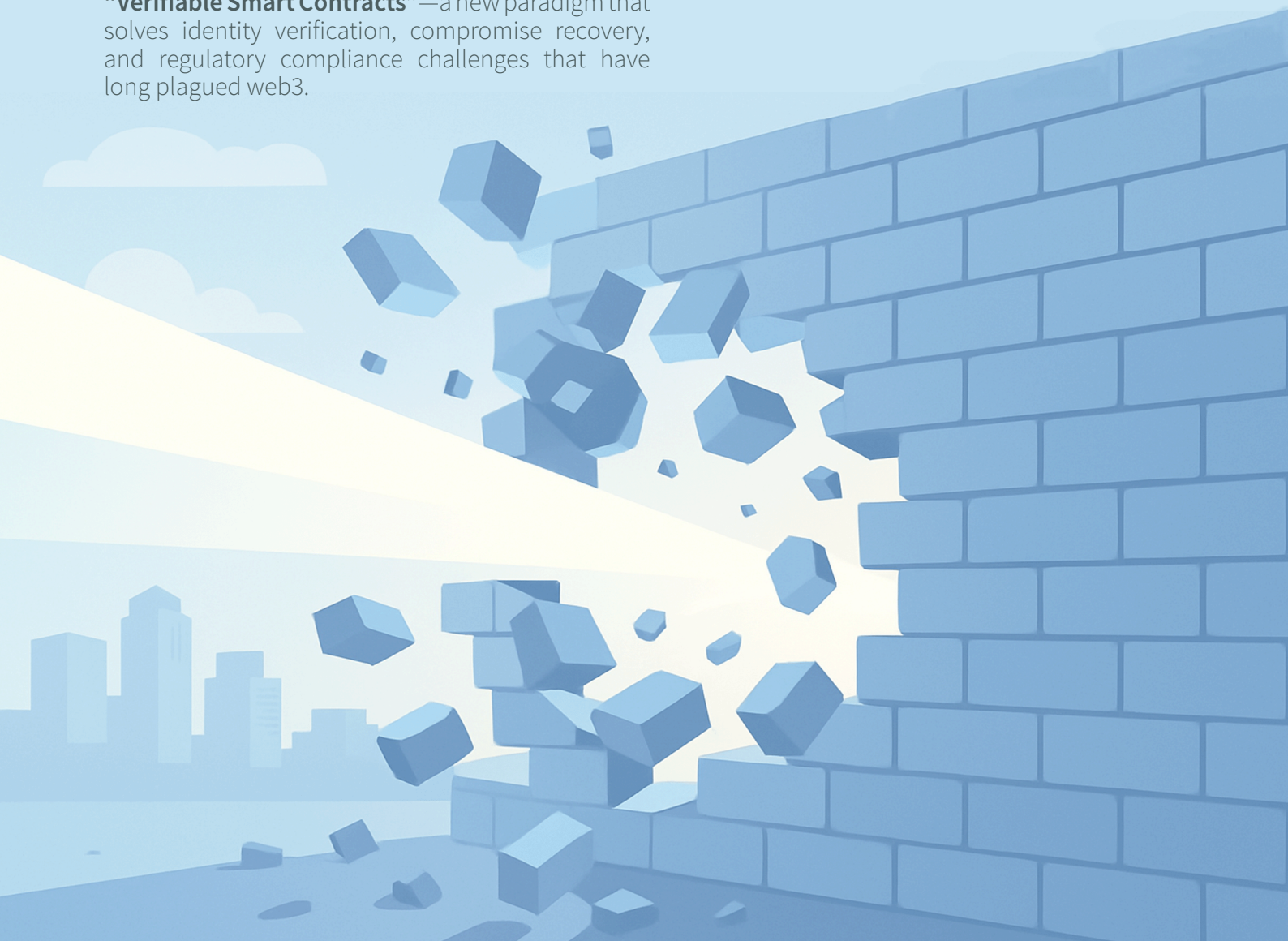
*The current state represents a critical inflection point: **either blockchain technology evolves to address these fundamental identity and recovery limitations, or it remains relegated to experimental use cases while traditional finance continues to dominate regulated activities.***

04.

The Breakthrough: vLEI & KERI

The fundamental limitations outlined above have persisted for over a decade, constraining blockchain adoption and creating billions in losses. However, **breakthrough innovations over the past three years have finally made comprehensive solutions possible.**

Two critical technological developments now provide the foundation to address these systemic problems: the maturation of **verifiable Legal Entity Identifiers (vLEI) through GLEIF's global infrastructure based on the Key Event Receipt Infrastructure (KERI) protocol** with its autonomic identifier capabilities. Together, these innovations enable the creation of **"Verifiable Smart Contracts"**—a new paradigm that solves identity verification, compromise recovery, and regulatory compliance challenges that have long plagued web3.



4.1 The vLEI

4.1.1 The Legal Entity Identifier (LEI): A Global Foundation of trust

The **Legal Entity Identifier (LEI)** is a 20-character ISO-standardized identifier created by the G20 in response to the 2008 financial crisis to uniquely identify legal entities worldwide. Administered by the Global Legal Entity Identifier Foundation (GLEIF)—a non-profit organization overseen by 70+ global regulators—the LEI system operates through a network of prestigious issuers including Bloomberg Finance, London Stock Exchange, Nasdaq, Tokyo Stock Exchange, and Swiss Federal Statistical Office.^[6]

The **LEI is mandatory** across numerous jurisdictions: required for all EU publicly traded companies, embedded in Universal Transaction Identifiers for banking (MiFID II/MiFIR), mandated by the US Financial Data Transparency Act, required by the CFTC for swap data reporting, mandated by the SEC for certain securities transactions, and many more globally. With over 2.9 million issued LEIs, it represents **the only globally recognized, persistent legal entity identifier** backed by G20 regulatory authority.^{[7][8][9]}

4.1.2 The verifiable LEI (vLEI)

In 2022, GLEIF introduced the verifiable LEI (vLEI), standardized under ISO 17442-3:2024, which transforms the static LEI into a **cryptographically verifiable digital credential**.

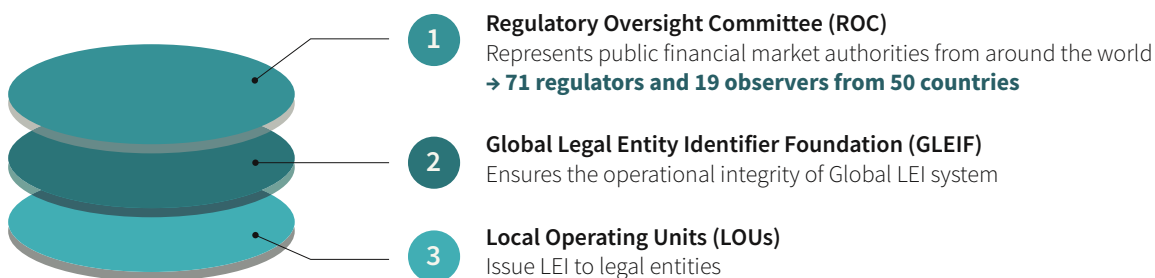
Built on the Key Event Receipt Infrastructure (KERI) protocol, **the vLEI enables organizations to create unforgeable digital signatures and issue unlimited sub-credentials for employees and roles.**^[10]

As the vLEI uses KERI, it does not require participants to onboard to a platform or blockchain and allows participants to use their own infrastructure.

Key vLEI capabilities:

- ◆ **Global Root of Trust:** GLEIF serves as the cryptographic anchor for organizational identity worldwide
- ◆ **Platform-Agnostic:** Unlike blockchain solutions, vLEI operates without requiring participants to join platforms, and allows users to use their own infrastructure
- ◆ **Infinite Delegation:** Organizations can issue role-based credentials (Official Organizational Role and Engagement Context Role) to any person or device
- ◆ **Cross-Border Verification:** Enables instant, automated verification of organizational identity and authority across jurisdictions
- ◆ **Highest possible security:** Compromise recovery without rotation of identifier - Quantum secure today

LEI Governance



For readers seeking comprehensive technical details on vLEI implementation and organizational identity infrastructure, we recommend:

"vLEI - The Rise of Organizational Digital Identity" (2025)
Key State Capital Report

→ An in-depth analysis of vLEI adoption patterns, technical architecture, and real-world implementation case studies across industries.

"Towards the Global Org eID System: Defining Requirements, Reviewing Regulations and Analyzing Technology Choices" (2025)
V. Suvorov, D. Saeuberli, C. Schneider, J. Buergi, D. Benz, A. Kech

→ A comprehensive examination of the LEI and vLEI intersection, regulatory frameworks, and the technical foundation for global organizational electronic identity systems.

"The vLEI: Introducing Digital I.D. for Organizations"
GLEIF eBook

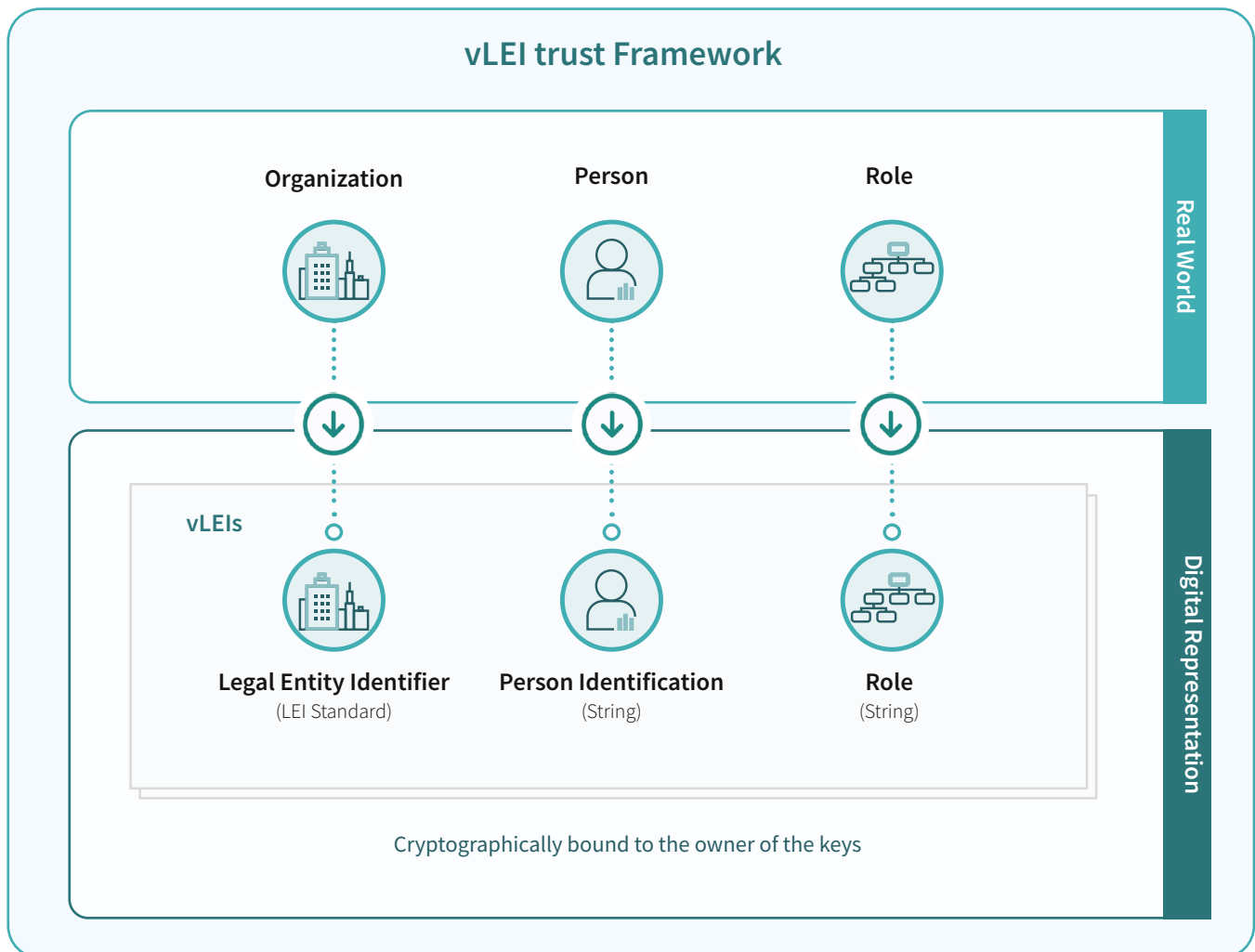
→ This eBook introduces the vLEI and the benefits it will bring to government agencies, companies, and other organizations worldwide.

These reports provide the detailed technical foundation and governance frameworks that underpin the verifiable smart contract solutions outlined in this analysis.

4.1.3 Binding Organization, Person and Role

The vLEI represents **the maturation of organizational digital identity**. It provides the missing cryptographic link between legal entities and their digital activities. This link enables smart contracts and automated systems to perform reliable verification.^[11]

While this report demonstrates the transformative potential of Verifiable Smart Contracts enabled by vLEI and KERI, exploring the detailed technical mechanisms of how the verifiable Legal Entity Identifier makes organizational digital identity a reality outside of web3 would exceed the scope of this analysis.



“By combining three concepts – the organization’s identity represented by the LEI, a person’s identity and the role that the person plays for the organization, vLEI credentials can be issued.”^[7]

4.2. Intro to KERI: the foundation of vLEI

Key Event Receipt Infrastructure (KERI) is a decentralized identity management protocol that forms the cryptographic foundation for **Verifiable Smart Contracts**. Unlike blockchain-based identity solutions, KERI uses a different architectural approach that addresses key limitations in digital identity and PKI systems.^[12]

Microledgers without global state

KERI's core design uses individual micro ledgers called Key Event Logs (KELs) for each autonomic identifier, rather than requiring global state consensus. Each entity controls its own Key Event Log, which records all cryptographic key management events for that identifier. This approach allows KERI-based identities to operate across different ecosystems without requiring participants to join specific blockchain networks.

→ Due to vLEI credentials being infinitely delegatable, every role in an organization can be represented.

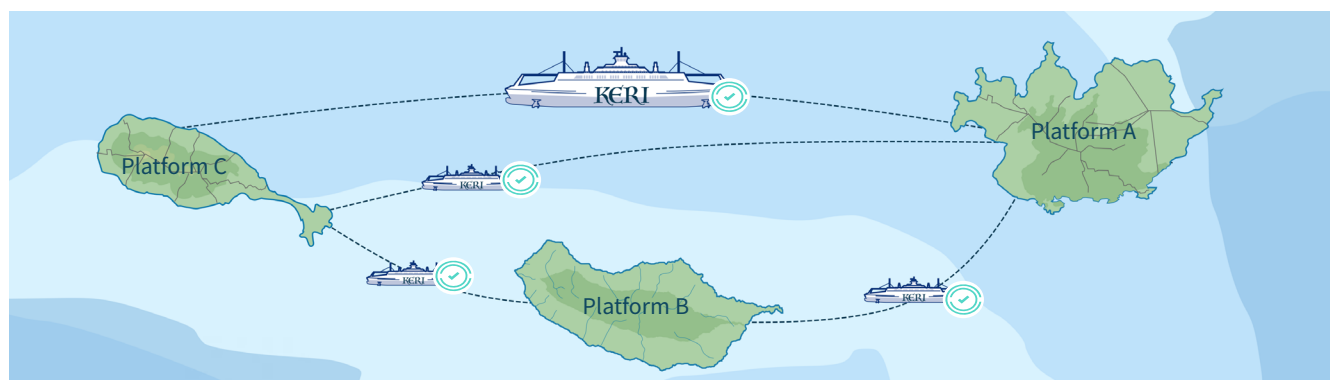
Key KERI capabilities:

- ◆ **Pre-Rotation Security:** Future cryptographic keys are committed in advance, enabling key updates without compromise risk during rotation periods
- ◆ **Compromise Recovery:** Entities can recover control of their identifiers after security breaches without requiring re-issuance of the identifier or requiring re-issuance of cryptographic assertions made in the past
- ◆ **Lifelong Self-Certifying Identifiers:** Identifiers remain valid and verifiable for an entity's entire lifetime without requiring maintenance from central authorities
- ◆ **Quantum-secure:** Identifiers created today remain secure after Q-Day
- ◆ **Verifiable Data Streams** at internet scale, facilitated by CESR (Composable Event Streaming Representation) encoding



Trust Domain Traversal

This micro ledger architecture enables verified organizational identity to move between different blockchains, enterprise systems, and regulatory frameworks. A vLEI credential issued in one ecosystem can be verified in any other ecosystem. The same organizational identity remains cryptographically verifiable whether operating on Ethereum, Cardano, or traditional enterprise systems.



KERI transports the trust GLEIF creates across platforms

05.

Overcoming the Limitations with Verifiable Smart Contracts

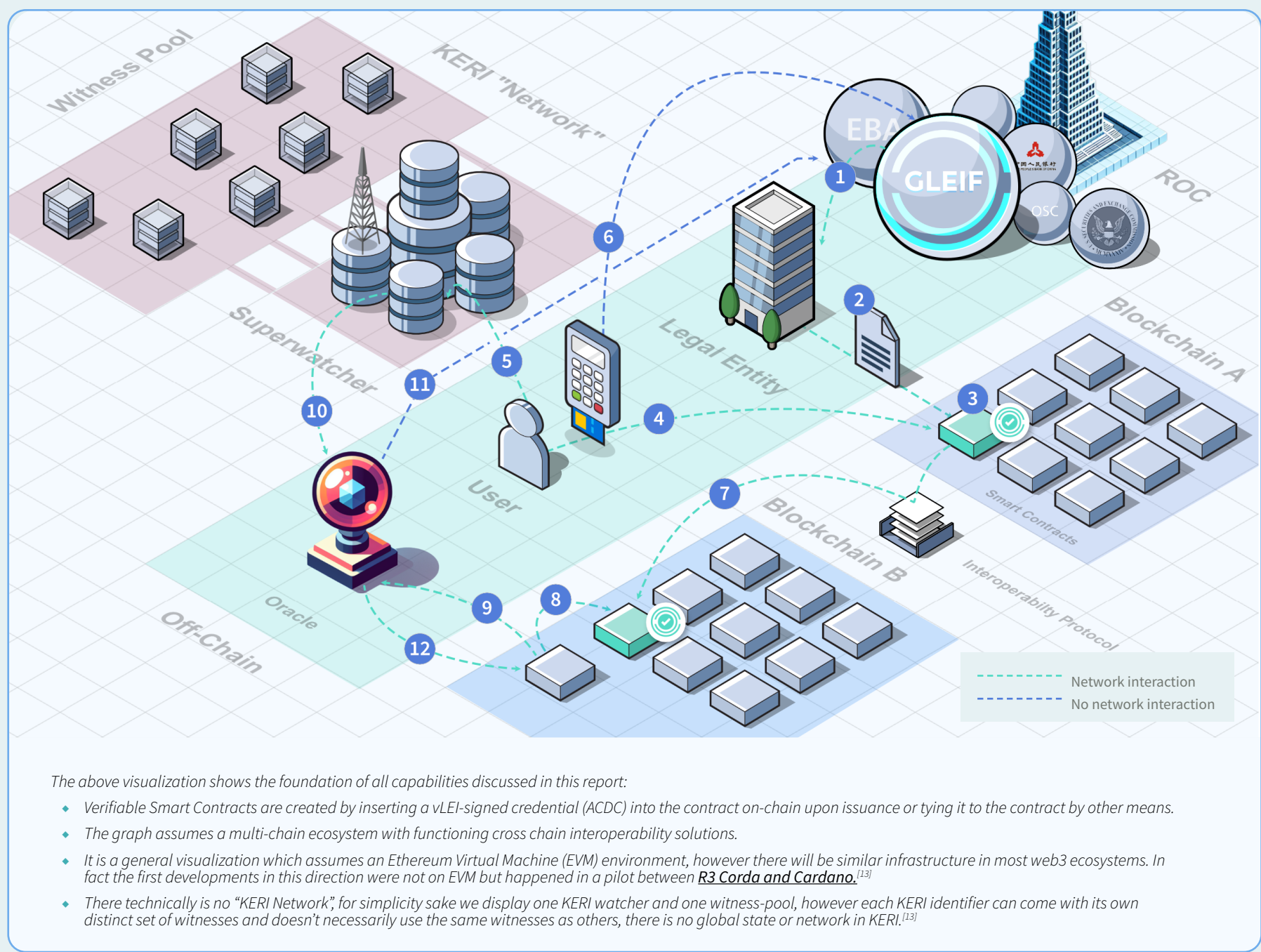
Verifiable Smart Contracts are:

- ◆ Provenanceable
- ◆ Compliant
- ◆ Verifiable off-chain
- ◆ Verifiable on-chain (only possible once watcher & oracle infrastructure is integrated)
- ◆ Capable of previously impossible security guarantees & failsafes

In the following pages, we go over several use-cases and capabilities Verifiable Smart Contracts will enable, which were previously impossible with traditional smart contracts.



How Verifiable Smart Contracts become real: A technical roadmap



Steps in Chronological Order:

- 1

Legal entity receives a vLEI (by undergoing a KYC/KYB onboarding ceremony with one of the Qualified vLEI issuers). This only happens once per entity.
- 2

The Legal entity which now is in possession of a vLEI, issues a smart contract and incorporates an ACDC (Authentic Chained Data Container) that contains a cryptographically verifiable assertion attesting to the legal entity being the issuer of this contract.
 - ♦ This can be any type of contract, such as a token.
 - ♦ It is undetermined what the best practices for inserting this data in an Ethereum Virtual Machine (EVM) context will be. The first-mover will likely set this standard.
- 3

The smart contract is **now verifiable by any party observing the on-chain data** as the ACDC is part of the blockchain's global state and can be discovered.
- 4

A user of the chain, in this example an individual with a wallet, can now verify provenance (verifiable issuance by the specific legal entity) with absolute certainty.
 - ♦ **This is immediately technically possible, even before oracles for vLEI signature verification on-chain are available.**
- 5

To execute this verification **off-chain**, the user's wallet or software:
 - ♦ Interacts with a KERI watcher or the KERI witnesses directly.
 - ♦ Discovers the up to date KEL (Key Event Log) which contains the current **KEY STATE** of the identifier (the vLEI of the issuing legal entity) which issued the ACDC that lives on-chain.
 - To achieve the full scope of KERI security, all signatures should be “anchored” in the KEL and an anchor should always be required in order for a signature to be considered valid.
- 6

The user verifies that:
 - ♦ The identifier has an unbroken chain of trust up to the Root of Trust (GLEIF)
 - This verification does not require a connection to any GLEIF infrastructure. This blue connection only represents the act of verifying cryptographic links to the root of trust, which involves communication with witnesses/watchers, but not with centralized GLEIF infrastructure.
 - ♦ The user can now be certain the smart contract was indeed issued from the legal entity that claims to issue it.
 - ♦ **Step 5&6 happen within seconds or milliseconds, and completely asynchronously from on-chain consensus.**
- 7

In a multi-chain world: The verifiable smart contract may be synced to multiple blockchains by existing cross-chain interoperability solutions. Given the ACDC is transmitted in this process, **the smart contract will remain verifiable off-chain as well as on-chain regardless of which method it gets discovered by.**
- 8

Another smart contract can verify the ACDC tied to the verifiable smart contract in order to make decisions based on the verification, if KERI-enabled Oracles exist.
- 9

Another smart contract attempts to verify the provenance of the verifiable smart contract, to do that it calls an oracle.
 - ♦ In order to verify the verifiable smart contract on-chain, additional infrastructure is needed:
 1. **An oracle** that can communicate with a KERI watcher in order to verify the vLEI's KEY STATE and subsequently verify the ACDC.
 - In order to deliver what is needed a “pull oracle”, which delivers information on demand is required. Oracle infrastructure already exists which can be adapted to serve this purpose. The needed adaptation is to be capable of step 10 (communicating with KERI infrastructure directly).
 2. **A “KERI watcher”:** Watchers are infrastructure from the KERI ecosystem, they monitor Key Event Logs of specific KERI autonomic identifiers on behalf of a verifier (the party wanting to verify claims made by a controller of an identifier). A KERI “superwatcher” or “global watcher” is a watcher which strives to observe all KELs instead of specifically watching KELs on demand.
 - While we did assume the existence of a Superwatcher in steps #5 and #6, the user in the example from steps #5 and #6 could have also verified the ACDC without it.
- 10

The oracle communicates with the KERI watchers in order to discover an up to date KEL (Key Event Log) which contains the current KEY STATE of the identifier (the vLEI of the legal entity that issued the token) which issued the ACDC that lives on-chain.
 - ♦ To achieve the full scope of KERI security, all signatures should be “anchored” in the KEL and an anchor should always be required in order for a signature to be considered valid.
- 11

The oracles then verify if the cryptographic chain of trust up to the root of trust (GLEIF) is unbroken
 - ♦ *This verification does not necessarily require a connection to any GLEIF infrastructure, this blue connection only represents the act of verifying the root of trust, which may involve communication with witnesses/watchers, but not with centralized GLEIF infrastructure.*
- 12

The Oracle then transmits the result of its verification back to the smart contract. **The smart contract can now make decisions based on this verification.**

5.1 Address Attribution: The end of whitelists

5.1.1 Current Limitations in Smart Contract Compliance

While smart contracts possess the theoretical capability to execute complex compliance checks, they face significant practical limitations due to insufficient access to counterparty information. This gap creates substantial barriers for businesses seeking to leverage blockchain technology for regulated activities and traps compliant RWA tokens in walled gardens.^[14]

Key Limitations:

- ✗ Smart contracts **lack access to identity information and credentials** that verify investor status
- ✗ **No access to identity data** that would enable proper compliance verification
- ✗ While Solidity functions can be written to perform compliance checks, **the underlying data required for these checks is unavailable or inconsistent**

5.1.2 The Tokenized Securities Challenge

Imagine a scenario where a small-to-medium enterprise (SME) decides to tokenize its shares utilizing the blockchain as a share registry. In theory, when shares require transfer, the smart contract managing the token could execute the necessary compliance checks automatically. However, **this theoretical capability breaks down in practice due to critical information gaps.**^[15]

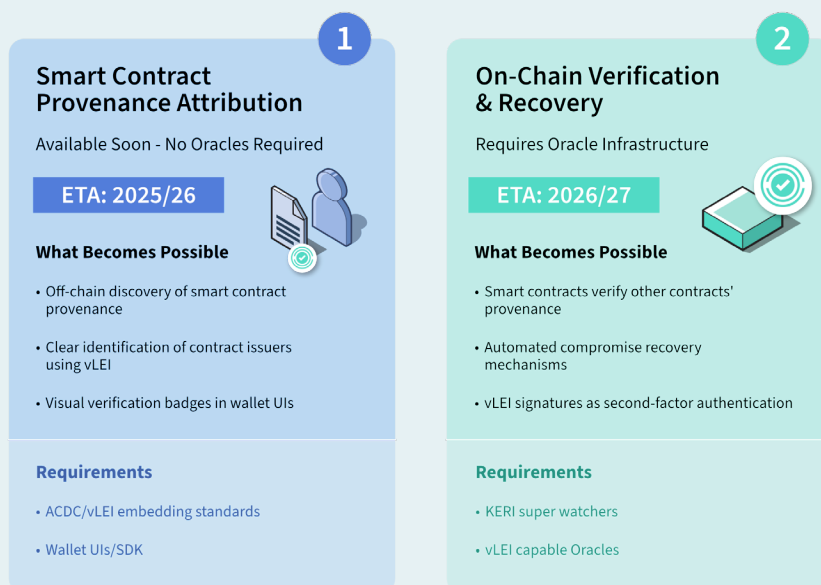
5.1.3 Current Market Reality

Due to these limitations, businesses tokenizing securities—whether SMEs or large corporations—are **currently constrained to operating through centralized security token exchanges**. These centralized platforms serve as the only viable option because they maintain the necessary infrastructure to perform compliance checks, such as:

- ◆ Verifying accredited investor status
- ◆ Conducting **know-your-customer (KYC)** procedures
- ◆ Ensuring **regulatory compliance across jurisdictions**
- ◆ Maintaining **audit trails for regulatory reporting**

5.1.4 The vLEI Solution - Verifiable Smart Contracts: A Two-Phase Evolution

The introduction of vLEI credentials presents a transformative opportunity to address these limitations through a structured, two-phase approach, with each phase building upon the previous one's capabilities.



Continues on the next page →

Phase 1: Smart Contract Provenance Attribution

Smart Contract Provenance Attribution

Available Soon - No Oracles Required

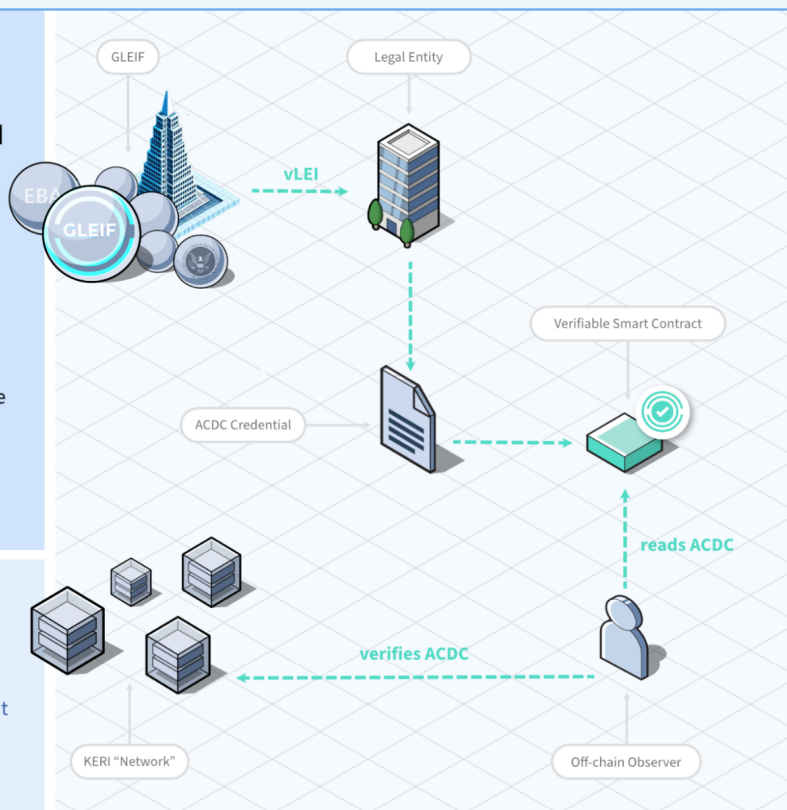
ETA: 2025/26

What Becomes Possible

- Enhanced transparency through embedded ACDC credentials
- Off-chain discovery of smart contract provenance
- Clear identification of contract issuers using vLEI
- Improved trust and accountability

Requirements

- Web3 consensus on ACDC embedding standards
- vLEI signature integration in contract deployment
- Wallet/UI updates to read embedded credentials



The initial phase focuses on establishing smart contract/address attribution, which serves as the foundational layer for enhanced smart contract functionality.

This phase will enable **enhanced transparency**:

- ◆ Embedding ACDC credentials directly into smart contracts to prove issuer identity
- ◆ Users and off-chain observers can discover the provenance of smart contracts without any doubt
- ◆ Clear identification of smart contract issuers using verifiable legal entity identifiers
- ◆ Improved trust and accountability in decentralized systems

Other Benefits:

- ◆ Increased confidence in smart contract interactions
- ◆ Better risk assessment capabilities for users
- ◆ Enhanced regulatory compliance through improved traceability
- ◆ Immediate implementation feasibility with current technology

As soon as a first-mover defines a common standard in which KERI ACDC verifiable credentials attesting to the vLEI of the issuing legal entity are to be tied to smart contracts, issuers of tokens will be able to cryptographically attest to their identity on-chain.

Any observer of the chain is then able to verify the provenance of a smart contract off-chain (step 1 through 6 on page 14).

Continues on the next page →

Phase 2: Inter-Contract Provenance Verification

On-Chain Verification & Recovery

Requires Oracle Infrastructure

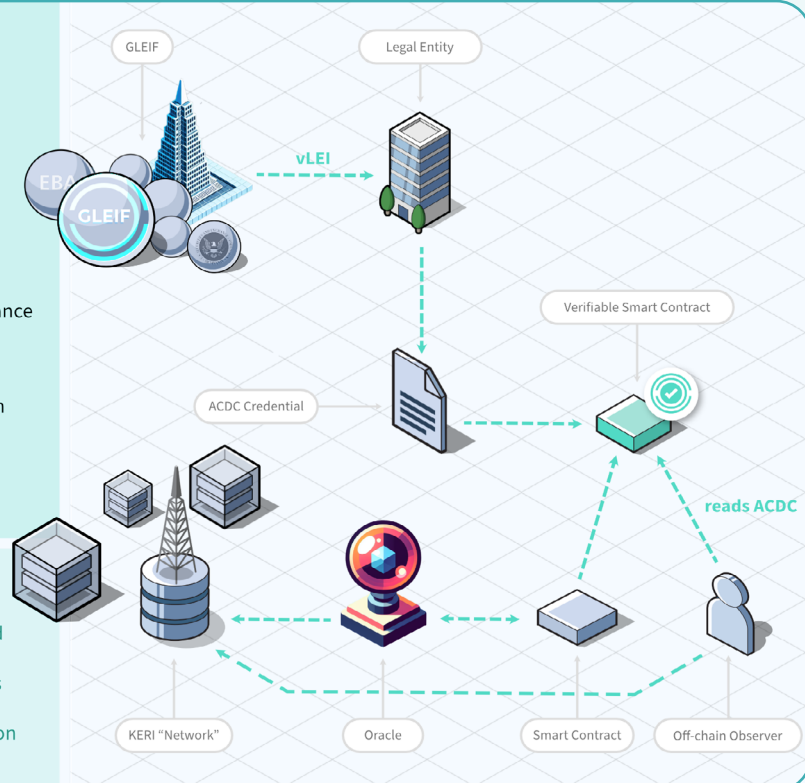
ETA: 2026/27

What Becomes Possible

- Smart contracts verify other contracts' provenance
- Automated compromise recovery mechanisms
- vLEI signatures as second-factor authentication
- Cross-contract trust establishment
- Real-time compliance

Requirements

- Global KERI watchers/super watchers deployed
- Oracle networks communicating with watchers
- Smart contract verification logic implementation



The second phase enables smart contracts to programmatically verify each other's credentials and provenance.

Oracle-Enabled Verification:

- ◆ Introduction of oracles capable of verifying embedded ACDC credentials (since smart contracts are incapable of communicating with off-chain infrastructure, oracles are required to contact KERI infrastructure on their behalf)
- ◆ Smart contracts can programmatically verify the provenance of other contracts they interact with
- ◆ Currently, this verification is only possible through manual whitelisting processes, which are static, centralized, and prone to human error
- ◆ vLEI-enabled smart contracts will perform real-time verification of counterpart contract credentials and issuer authenticity
- ◆ Automated trust establishment between smart contracts based on verifiable provenance data

Implementation Advantages:

- ◆ No privacy concerns as only organizational credentials are involved and all credentials involved are meant to be public
- ◆ Immediate benefits for institutional and enterprise use cases

With a KERI watcher-Oracle available, smart contracts can autonomously check the provenance and controlling legal entity behind a smart contract on-chain (step 1-3 & 7-12 on page 14).

Continues on the next page →

Long-Term Additional Use Cases: Individual Credential Integration

After phase 1 & 2 are realized the most complex evolution which enables individuals to provide verifiable credentials directly to smart contracts for compliance purposes may become viable.

Individual Credential Capabilities:

- ◆ Users can provide verifiable credentials directly to smart contracts on-chain
- ◆ Automated compliance checks based on verified identity attributes, such as accredited investor status
- ◆ Enhanced privacy through selective disclosure of credentials

Privacy Concerns and Limitations:

- ◆ Privacy challenges exist when individuals provide verifiable credentials to smart contracts
- ◆ Current solutions do not adequately address privacy protection for personal credential disclosure
- ◆ These privacy concerns require substantial additional research and development

Future Applications Examples:

- ◆ Automated accredited investor verification for tokenized securities
- ◆ Real-time compliance checking for regulated transactions involving individuals
- ◆ Enhanced privacy through selective disclosure of credentials (when privacy solutions are developed)

5.1.5 Impact on the Tokenized Securities Market

This two-phase evolution will fundamentally transform how tokenized securities operate, with immediate benefits available from Phases 1 and 2:

Immediate Decentralization Benefits (Phases 1 & 2):

- ◆ Enhanced trust and transparency through verifiable smart contract provenance
- ◆ Automated verification between institutional smart contracts
- ◆ Dynamic smart contract interaction policies based on verified organizational provenance
- ◆ Reduced reliance on manual whitelisting processes

Future Individual Benefits:

- ◆ Reduced dependence on centralized security token exchanges for individual investors
- ◆ Direct peer-to-peer trading with automated compliance for retail participants
- ◆ Lower transaction costs and increased market efficiency for all participants
- ◆ Greater accessibility for individual investors to participate in tokenized securities

Regulatory Advantages:

- ◆ Improved compliance monitoring and reporting capabilities
- ◆ Real-time regulatory oversight of institutional interactions
- ◆ Enhanced investor protection through verified organizational credentials
- ◆ Standardized compliance frameworks across jurisdictions
- ◆ Clear provenance tracking for all smart contract interactions

5.1.6 Conclusion

Address attribution represents the critical first step toward enabling truly decentralized, compliant smart contract ecosystems. The two-phase evolution provides a realistic roadmap where Phases 1 and 2 can be implemented in the short term to establish organizational trust and inter-contract verification.

By establishing clear organizational provenance and enabling automated verification between institutional smart contracts, vLEI credentials will unlock significant potential for regulated activities in the tokenized securities market. This measured approach ensures that immediate benefits can be realized while acknowledging the complex privacy challenges that must be solved before full individual participation becomes viable. The evolution promises to democratize access to capital markets while maintaining the highest standards of regulatory compliance and organizational accountability.

5.2. De-Fi Fraud prevention

Even without a KERI watcher oracle available, as outlined in 5.1.4 phase 1, **ACDC attestations tied to smart contracts will enable wallets and other UIs to display information about tokens' provenance and reduce fraud.**

5.2.1 The Current Token Fraud Crisis

The decentralized finance (DeFi) ecosystem faces a persistent and growing threat from **fraudulent tokens and malicious smart contracts**. Scammers routinely create fake versions of legitimate tokens by exploiting blockchain's open nature—anyone can deploy smart contracts with identical names, symbols, and visual appearance but completely different contract addresses and malicious functionality. These scammers then trick victims into using fake tokens through phishing websites, fake airdrops, social media impersonation, or by manipulating search results to promote fraudulent contract addresses. **This fundamental security challenge undermines trust in the DeFi ecosystem and creates significant barriers to mainstream adoption.**^[16]

5.2.2 The Scale of the Problem

Consider the widespread proliferation of fraudulent stablecoins. For every legitimate token like USDC, thousands of scam tokens exist with identical or similar names, designed to deceive users into believing they are interacting with the authentic asset. **These fraudulent tokens represent one of the most significant threats to DeFi users**, particularly newcomers who lack the technical expertise to verify token authenticity.

5.2.3 Common On-Chain Fraud Examples:

❗ Token Impersonation Attacks:

- ◆ Fake versions of popular tokens (USDT, USDC, DAI) with nearly identical names or symbols
- ◆ Users unknowingly purchase worthless tokens believing they are buying legitimate assets

❗ Rug Pull Schemes:

- ◆ Projects launch tokens with professional-looking websites and marketing materials
- ◆ Developers drain liquidity pools or abandon projects after collecting investor funds
- ◆ No way for users to verify the legitimacy of the development team or company behind the token

❗ Honeypot Tokens:

- ◆ Malicious smart contracts that allow users to buy tokens but prevent them from selling
- ◆ Contract code appears legitimate on the surface but contains hidden restrictions
- ◆ Users lose funds when they cannot exit their positions

❗ Phishing Through Fake Airdrops:

- ◆ Scammers create tokens with names suggesting they are airdrops from legitimate projects
- ◆ Users interact with malicious contracts thinking they are claiming free tokens
- ◆ These interactions often result in wallet drains or approval exploits

❗ Cross-Chain Bridge Exploits:

- ◆ Fake wrapped tokens claiming to represent assets from other blockchains
- ◆ Users bridge assets to receive worthless tokens instead of legitimate wrapped versions
- ◆ No standardized way to verify the authenticity of cross-chain token representations

❗ Example of Token Impersonation Attacks:

Txn Hash	Date Time (UTC)	From	To	Value	Token
0x67d215c74f86f5ff92...	2023-03-22 11:50:35	0xeb6454...84fE1ed8	OUT 0x69a949...C24Df0f8	206,660.150445	ERC-20: Tet....DT)
0x67d215c74f86f5ff92...	2023-03-22 11:50:35	0xeb6454...84fE1ed8	OUT 0x2F682...F1705E78	6,000	ERC-20: Tet....DT)
0x67294b75afa3ac...	2023-03-21 8:48:11	0xeb6454...84fE1ed8 User's own address	OUT 0x2f10...f1C05E78 Fake address with similar first and last characters	Same quantity	Tether USD (USDT)
0x8422f896a121450b2...	2023-03-21 8:36:35	0xeb6454...84fE1ed8	OUT 0x2F6a86...30c05e78	6,000	Fake USDT ERC-20: Tet....DT)
0x231fee5dcd76cfe5b...	2023-03-21 8:07:11	0xeb6454...84fE1ed8 Genuine address	OUT 0x2f682D...78C05e78	6,000	Real USDT Tether USD (USDT)

Source: imToken

This scam involves fake USDT transactions that appear real by using a phishing contract which mimics a legitimate token, and wallet addresses designed to mimic the user's own, tricking them into sending funds to the scammer^[17]. With Verifiable smart Contracts, the legitimate contract could be easily differentiated in the UI.

5.2.4 Current Verification Methods: Inadequate and Insecure

Today's token verification methods are fundamentally flawed and rely on centralized, error-prone processes:

Manual Verification Processes:

- ♦ Users must manually search for official contract addresses, i.e. through Google searches
- ♦ Verification requires cross-referencing multiple sources including official websites and social media accounts
- ♦ Users must hope that the information they find matches the actual legitimate contract address

→ *This process is time-consuming, unreliable, and accessible only to technically sophisticated users.*

Wallet Hard-coding:

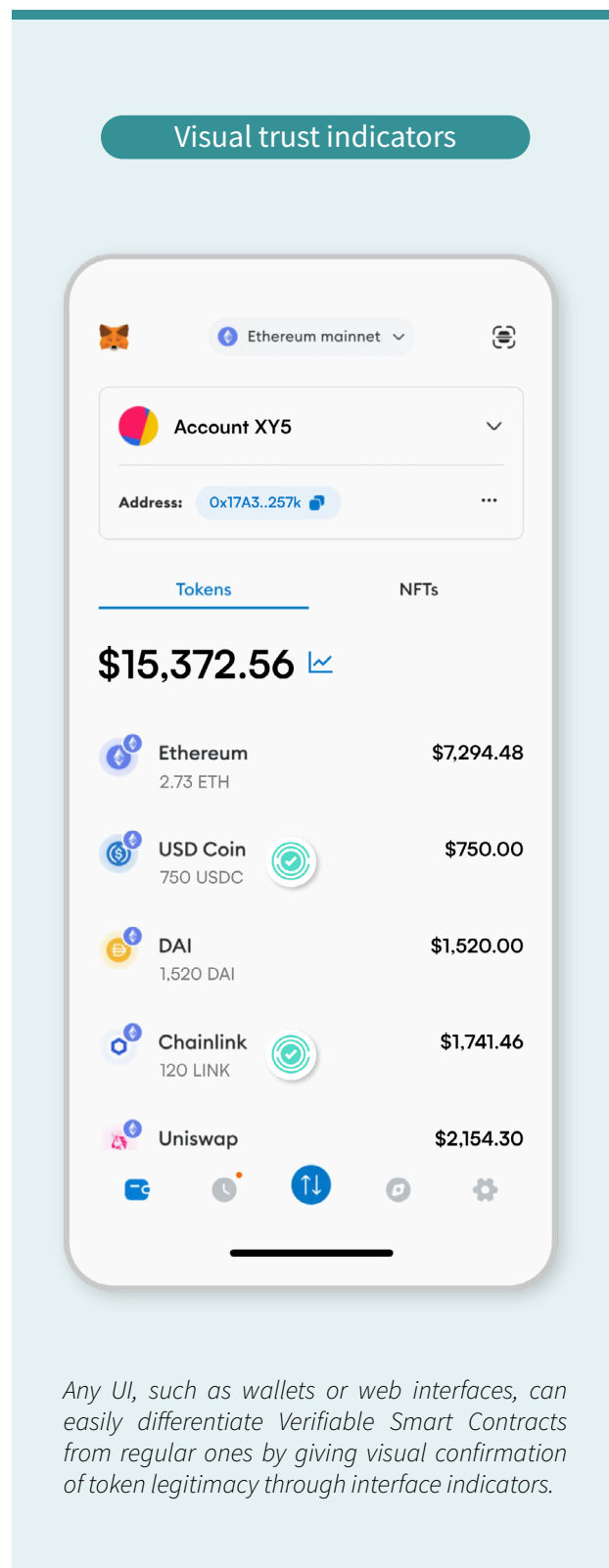
- ♦ Major wallets pre-program popular token contracts into their systems
- ♦ While this provides some protection for well-known tokens, it creates a centralized point of failure
- ♦ New or lesser-known legitimate tokens cannot benefit from this protection
- ♦ The hard-coding process itself is manual and subject to human error and provides attack-surface

Fundamental Security Flaws:

- ♦ No cryptographic verification of token authenticity
- ♦ Reliance on external, potentially compromised information sources
- ♦ Vulnerability to sophisticated phishing attacks that mimic official sources
- ♦ Inability to verify the legitimacy of new or emerging tokens

5.2.5 Solution: Verifiable Smart Contracts - Cryptographic Token Authentication

The integration of vLEI credentials with smart contracts presents a transformative solution to the token fraud epidemic. By enabling token issuers to attach ACDC credentials that attest their vLEI to specific smart contracts, the system creates an unbreakable cryptographic link between legal entities and their issued tokens.



Any UI, such as wallets or web interfaces, can easily differentiate Verifiable Smart Contracts from regular ones by giving visual confirmation of token legitimacy through interface indicators.

5.2.6 How vLEI Token Authentication Works

Cryptographic Binding:

The technical process of attaching vLEI credentials to smart contracts is detailed in Section 4 & 4a (Address Attribution).

In summary:

- ◆ Token issuers **attach ACDC credentials to their smart contracts** during deployment
- ◆ These **credentials cryptographically link the smart contract to a specific legal entity** through their vLEI
- ◆ The binding creates an **immutable, verifiable connection** between the issuer's legal identity and their token
- ◆ This process establishes provenance that can be verified by wallets and (once oracles are available) other smart contracts

Wallet-Level Verification:

- ◆ Wallets can programmatically verify the authenticity of smart contracts in real-time
- ◆ Users receive immediate visual confirmation of token legitimacy through interface indicators
- ◆ Verification occurs automatically without requiring manual user intervention

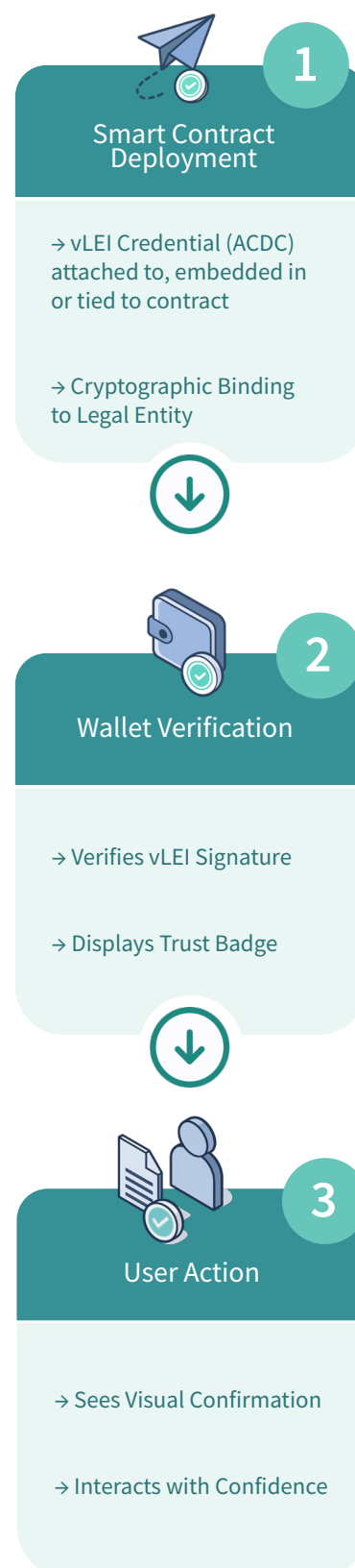
5.2.7 User Experience Transformation

Visual Trust Indicators:

- ◆ Wallets will display clear verification badges (such as checkmarks) for vLEI-verified smart contracts, similar to the https lock in browsers (except it's actually secure)
- ◆ Users can instantly distinguish between verified and unverified tokens
- ◆ Advanced users can examine the specific vLEI attached to any smart contract for detailed verification

Simplified Due Diligence:

- ◆ The presence of a vLEI signature serves as an immediate quality indicator
- ◆ Users no longer need to perform complex manual verification processes
- ◆ Trust establishment becomes instantaneous and cryptographically secure



5.2.8 Fraud Prevention Mechanisms

KYC Requirements:

- ◆ Obtaining a vLEI requires completing rigorous Know Your Customer/Business (KYC/KYB) procedures
- ◆ Scammers cannot easily impersonate legitimate entities due to identity verification requirements
- ◆ The cost and complexity of obtaining fraudulent vLEI credentials creates a significant barrier to entry for malicious actors

Legal Accountability:

- ◆ vLEI signatures create clear legal trails linking smart contracts to real-world entities
- ◆ Fraudulent use of vLEI credentials carries severe legal consequences
- ◆ Regulatory authorities can easily identify and pursue bad actors

5.2.9 Elimination of Common Attack Vectors

Name Impersonation Prevention:

- ◆ Scammers can no longer rely solely on similar token names to deceive users
- ◆ Visual verification indicators immediately expose fraudulent tokens lacking proper credentials
- ◆ Users develop trust patterns based on cryptographic verification rather than superficial similarities

Phishing Attack Mitigation:

- ◆ Fake websites and social media accounts become ineffective when users rely on cryptographic verification
- ◆ The verification process occurs within the wallet interface, eliminating external dependencies
- ◆ Users no longer need to navigate potentially compromised external verification sources

5.2.10 Market Impact and Adoption Incentives

Competitive Advantages for Legitimate Projects

- ◆ **Trust Premium:**
Projects with vLEI verification will enjoy enhanced user confidence and adoption and verified tokens will command premium positioning in wallet interfaces and DeFi platforms. Market forces will incentivize legitimate projects to obtain vLEI credentials
- ◆ **Reduced Support Burden:**
Projects will experience fewer user inquiries about token authenticity and customer support resources can focus on product development rather than fraud prevention. The enhanced user experience leads to improved retention and growth

5.2.11 Ecosystem-Wide Benefits

Platform Integration:

- ◆ DeFi platforms can implement automatic filtering based on vLEI verification status
- ◆ Exchanges can offer enhanced security tiers for verified tokens
- ◆ Aggregators can prioritize verified tokens in their interfaces

Regulatory Compliance:

- ◆ vLEI verification supports regulatory compliance efforts across jurisdictions
- ◆ Clear audit trails facilitate regulatory reporting and oversight
- ◆ Enhanced transparency supports institutional adoption of DeFi protocols

5.2.12 Conclusion

vLEI-based token authentication represents a paradigm shift in DeFi security, transforming fraud prevention from a reactive, manual process to a proactive, cryptographically secure system. By creating unbreakable links between legal entities and their issued tokens, this approach will dramatically reduce the success rate of token fraud while enhancing user confidence in the DeFi ecosystem.

The implementation of vLEI based **Verifiable Smart Contracts** will create a clear distinction between legitimate, verified tokens and potentially fraudulent alternatives. This distinction will drive market forces toward greater transparency and accountability, ultimately fostering a more secure and trustworthy decentralized financial system. As adoption grows, users will benefit from simplified due diligence processes, enhanced security, and greater confidence in their DeFi interactions.

The implementation of vLEI based Verifiable Smart Contracts will create a clear distinction between legitimate, verified tokens and potentially fraudulent alternatives.

5.3. Compromise Recovery

*On a long enough timeline, **all actively used cryptographic keys will eventually be compromised through various attack vectors** including phishing, malware, insider threats, sophisticated state-level attacks, or surprise quantum attack.*

Imagine if losing your house keys meant you could never enter your home again—even if you could prove you own the house, show your deed, and have your neighbors vouch for you. This is exactly what happens in today’s blockchain world when cryptographic keys get compromised.

In traditional smart contracts, **once a hacker steals your private keys, they own your contract forever**. There’s no “calling the locksmith” or “proving your identity to get back in.” The stolen keys work perfectly, and the blockchain can’t tell the difference between you and the attacker.

Think about how recovery works in the real world. If a company’s CFO loses their laptop, they don’t lose access to the company bank account forever. Instead, the CEO can authorize new access, the board can override decisions, or the company can follow established recovery procedures.

Verifiable Smart Contracts will enable the same type of organizational recovery for smart contracts. Instead of tying control to specific digital keys that can be stolen, smart contracts can recognize legitimate organizational roles and authority.

5.3.1 The Inevitability of Key Compromise

In blockchain systems, the security assumption that private keys can remain secure indefinitely is fundamentally flawed. On a long enough timeline, all actively used cryptographic keys will eventually be compromised through various attack vectors including phishing, malware, insider threats, sophisticated state-level attacks, or surprise quantum attack. This reality creates a critical vulnerability in traditional smart contract architectures where key compromise results in permanent loss of control and assets.

5.3.2 The vLEI Solution: Perpetual Recovery Capability

vLEI credentials integrated with KERI infrastructure provide a revolutionary solution to the key compromise problem through perpetual recovery mechanisms that remain valid indefinitely.

5.3.3 Legal Entity-Based Recovery Rules

Once vLEI enabled web3 oracles exist, smart contracts can implement recovery logic based on verifiable legal entity roles rather than specific cryptographic keys:

Example Recovery Rule:

“The CEO of Entity XYZ with LEI 1234 can always call transferOwnership()”

This rule enables legitimate organizational representatives to regain control of compromised contracts by proving their authorized status through vLEI credentials, regardless of when the compromise occurred.

Flexible Authorization Models:

- ◆ Single executive authorization (CEO, CTO, etc.)
- ◆ Multi-signature board member requirements
- ◆ Specific organizational role combinations
- ◆ Time-based or conditional authorization schemes

5.3.4 Two-Tier Recovery Architecture

Tier 1: Ownership Recovery

The foundational recovery mechanism allows authorized personnel to regain control of compromised smart contracts:

Process:

1. Authorized representative presents vLEI credential proving their role
2. Smart contract verifies the credential against the embedded legal entity rules, using a vLEI capable Oracle for discovering KEY STATE
3. Upon successful verification, ownership transfers to a new, secure address
4. Legitimate control is restored, and the compromised keys are invalidated

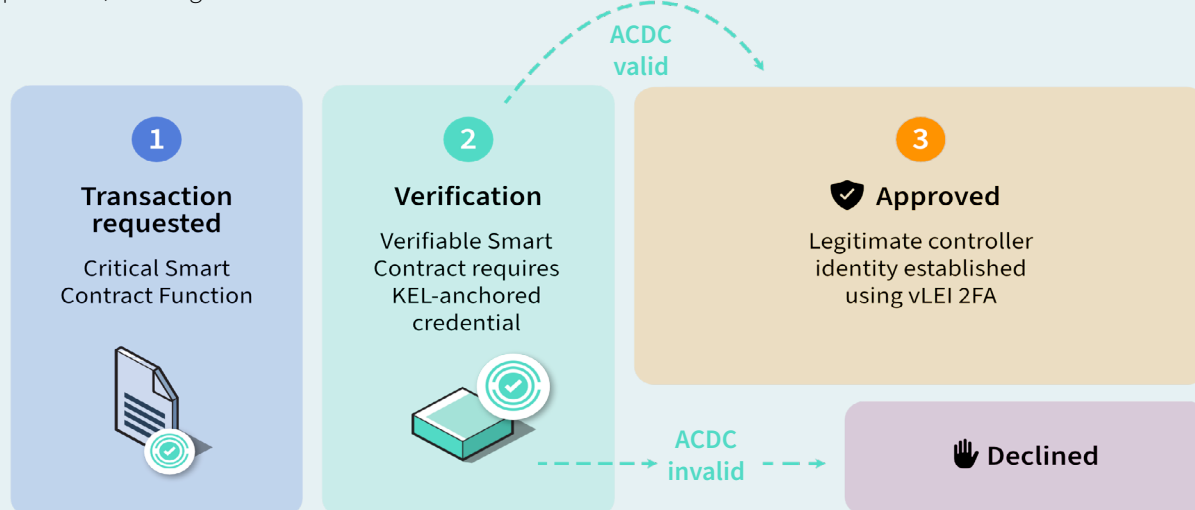
Benefits:

- ◆ Immediate restoration of legitimate control
- ◆ Invalidation of attacker access
- ◆ Preservation of contract functionality and trust
- ◆ Low-cost: oracle cost only incurred when recovery is needed



Tier 2: Transaction-Level Protection

An advanced implementation (proposed by Dr. Samuel Smith, KERI originator) requires vLEI signatures for critical operations, creating a second factor of authentication:



Enhanced Security Model:

Critical functions (fund transfers, parameter changes) require dual authorization

1. **Primary authorization:** Traditional private key signature.
2. **Secondary authorization:** KERI-KEL-anchored vLEI signature from the legal entity's key event log.

Attack Resistance:

Even if an attacker compromises the primary private keys, they cannot execute critical functions without also controlling the legal entity's vLEI credentials and KERI infrastructure access.

Key Rotation Without Identifier Change:

Legal entity identifiers remain constant even after key compromises, allowing new keys to be rotated in on the vLEI AID without updating smart contract rules. This ensures recovery and the breach prevention mechanisms in tier 1 & 2 remain valid indefinitely, providing seamless continuity without disrupting existing smart contract infrastructure.



5.3.5 Technical Implementation Requirements

Oracle Infrastructure

vLEI Oracle/ KERI watcher Requirements:

- ◆ Real-time resolution of KERI key state
- ◆ Verification of key event logs and credential validity
- ◆ Integration with smart contract verification logic

Verification Process:

1. Smart contract receives recovery request with vLEI credential
2. Oracle resolves current key state from KERI infrastructure
3. Credential authenticity verified against legal entity's key event log
4. Authorization confirmed based on embedded recovery rules

Smart Contract Integration

Potential recovery Rule Implementation:

- ◆ Hardcoded legal entity-based authorization rules
- ◆ Multi-signature support for board-level decisions
- ◆ Time-lock mechanisms for additional security
- ◆ Event logging for audit and compliance purposes

Anchored Event Verification:

- ◆ Critical operations requires events in the legal entity's key event log
- ◆ Smart contracts verify these anchored events before execution
- ◆ Dual-factor authentication through traditional keys plus vLEI signatures

→ In order to trigger a malicious transaction, the attacker needs to not only compromise the on-chain private key, but also the vLEIs controller key (which can recover from compromise due to KERIs features).

→ As the requirement is a KEL-anchored event, the attacker then even has to publicly announce his intention of making a transaction before he can try to trigger an action on-chain.

5.3.6 Security and Trust Implications

Enhanced Security Model

Multi-Layer Protection:

The security model combines traditional cryptographic security for routine operations with legal entity verification for critical functions and recovery. KERI infrastructure provides quantum-resistant foundations while organizational governance is seamlessly integrated into technical security, creating a comprehensive defense system.

Attack Vector Mitigation:

Key compromise doesn't result in permanent loss, while social engineering attacks require both technical and legal entity compromise to succeed. Insider threats are mitigated through multi-signature requirements, and state-level attacks require compromise of both technical and legal infrastructure, making the system resilient against even sophisticated adversaries.

Trust Preservation

Continuous Legitimacy:

- ◆ Legitimate owners can always regain control
- ◆ Trust in the system survives individual key compromises
- ◆ Legal entity backing provides additional trust anchors
- ◆ Regulatory compliance maintained through verifiable organizational control

5.3.7 Use Cases and Applications

Enterprise Smart Contract Management

Corporate Treasury Management:

- ◆ Multi-signature board control with individual recovery rights
- ◆ CEO emergency access for critical business decisions
- ◆ Compliance officer oversight for regulatory requirements
- ◆ Audit trail through legal entity key event logs

Tokenized Asset Management:

- ◆ Issuer control preservation across security incidents
- ◆ Regulatory compliance through verifiable entity control
- ◆ Investor protection through legitimate issuer verification
- ◆ Market confidence through perpetual recovery capability



5.3.8 Conclusion

Compromise recovery through vLEI represents a fundamental advancement in smart contract security architecture. By anchoring recovery mechanisms to verifiable legal entity credentials rather than specific cryptographic keys, this approach solves the critical problem of permanent loss following key compromise.

The perpetual nature of KERI-based vLEI credentials ensures that recovery capabilities remain valid indefinitely, requiring no maintenance or updates to smart contract rules. This creates a robust security model where legitimate organizational control can always be restored, regardless of the scale or timing of security breaches.

This capability transforms smart contracts from fragile, single-point-of-failure systems into resilient, enterprise-grade infrastructure capable of surviving the inevitable reality of key compromise while maintaining trust, functionality, and regulatory compliance.

5.4. Compliance: Travel Rule Protocol example

5.4.1 The FATF Travel Rule and Current Implementation Challenges

The Financial Action Task Force (FATF) Travel Rule represents one of the most significant compliance requirements facing the cryptocurrency industry today. Mandated by regulations such as the Markets in Crypto-Assets (MiCA) regulation in Europe, the Travel Rule requires Virtual Asset Service Providers (VASPs) to exchange Know Your Customer (KYC) information about their clients before executing transactions between different VASPs.^{[18][19]}

Travel Rule Requirements

Core Mandate:

When a VASP transmits virtual assets on behalf of a client to another VASP, both parties must:

- ◆ Exchange KYC information about the originating client
- ◆ Receive and verify KYC information about the beneficiary client
- ◆ Complete this information exchange before executing the transaction
- ◆ Maintain compliance records for regulatory reporting

Current Technical Implementation:

The cryptocurrency industry has converged on two primary technical standards:

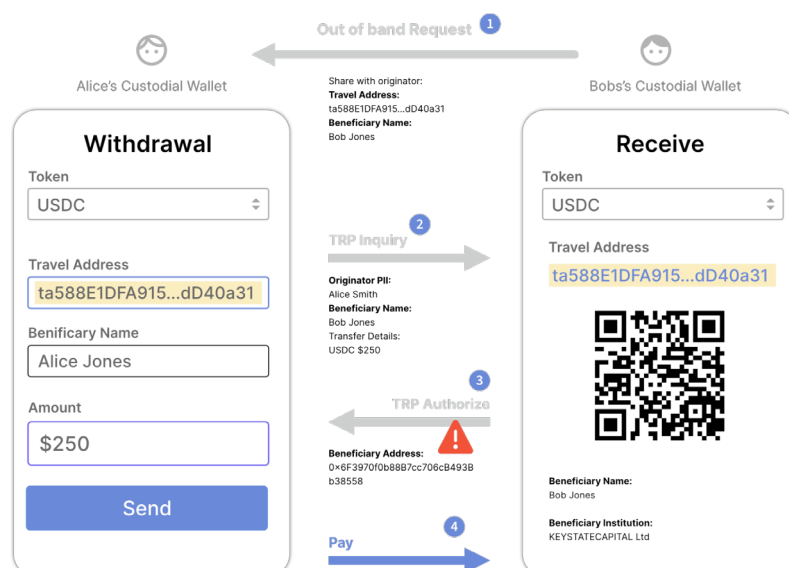
1. **InterVASP Messaging Standard (IVMS):** Defines the data payload format for KYC information exchange^[20]
2. **Travel Rule Protocol (TRP):** Developed by OpenVASP, provides the communication mechanism for information exchange^[21]

Current Implementation Vulnerabilities

The existing Travel Rule implementation contains critical security flaws that create significant risks for all participants.

Insecure URL-Based Communication - Process Flow

- 1 **Out-of-Band Request:** Bob provides Alice with a “travel address” that looks to like a cryptocurrency address visually but is actually an encoded API endpoint (e.g., exampleVASP-a.com/trp?uid=1337)
- 2 **VASP Inquiry:** Alice’s VASP sends a Travel Rule Protocol inquiry to this API endpoint, transmitting:
 - ◆ Personal information about Alice
 - ◆ The originating VASP’s Legal Entity Identifier (LEI)
 - ◆ Transaction details
- 3 **Compliance Verification:** Bob’s VASP performs sanctions checks and compliance verification
- 4 **Authorization Response:** If approved, Bob’s VASP responds with:
 - ◆ Travel Rule Protocol authorization
 - ◆ The actual on-chain address for fund transfer
 - ◆ Beneficiary information





5.4.2 Critical Security Vulnerabilities in Travel Rule Protocol

User-Controlled URL Vulnerability:

- ◆ The API endpoint URL is controlled by the user (Bob) and transmitted through insecure channels
- ◆ Malicious actors can easily substitute fraudulent endpoints
- ◆ Originating VASPs may unknowingly send sensitive customer data to attacker-controlled servers

→ *The only countermeasure is whitelisting VASPs certs, which impacts interoperability and doesn't solve the weak TLS security used.* ^[22]

Legacy TLS Downgrade Attack:

- ◆ Critical customer data is transmitted over legacy PKI/TLS connections
- ◆ These systems are vulnerable to known certificate authority compromises

→ *The secure, self-certifying Bitcoin address gets downgraded to TLS-level security.*

Man-in-the-Middle Attack Surface:

Attackers gaining control of the API endpoint (even temporarily) can:

- ◆ Replace the legitimate receiving address with an attacker-controlled address
- ◆ Steal large amounts of funds by redirecting transactions
- ◆ Harvest sensitive customer KYC data

A Regulator-Mandated Honeypot:

- ◆ Regulators are inadvertently forcing the entire cryptocurrency industry to adopt this insecure protocol or centralized alternatives
- ◆ The mandatory nature creates a massive attack surface that bad actors can and will systematically exploit
- ◆ All institutional participants must follow this protocol, creating universal vulnerability

Alternative Solutions and Their Limitations

While some alternative solutions exist that don't use the Travel Rule Protocol, they all suffer from the same fundamental security problems or rely on centralized platforms:

- ◆ **Centralized Compliance Platforms:** Some VASPs use centralized third-party services for Travel Rule compliance, but these create single points of failure and still rely on insecure TLS communications
- ◆ **Proprietary Messaging Systems:** Custom bilateral agreements between VASPs often use proprietary protocols, but these still depend on traditional PKI/TLS security and lack standardization
- ◆ **Blockchain-Based Solutions:** Some attempts to put Travel Rule data on-chain exist, but without proper identity verification, they cannot solve the fundamental problem of verifying counterparty legitimacy
- ◆ **Manual Verification Processes:** Some institutions rely on manual, out-of-band verification, but this is slow, expensive, and doesn't scale for high-volume operations

→ *All of these alternatives either maintain the same security vulnerabilities as the standard Travel Rule Protocol or introduce centralization that defeats the purpose of decentralized finance.*

5.4.3 The Verifiable Smart Contract Solution: Enhanced Security through Smart Contract Attribution

The integration of vLEI credentials with smart contracts provides a revolutionary solution to Travel Rule security vulnerabilities by enabling cryptographic verification of receiving addresses.

Secure Implementation Process:

1. **vLEI-Verified Smart Contracts:** Receiving addresses are tied to Verifiable Smart Contracts that contain embedded vLEI credentials.
2. **Cryptographic Address Verification:** Before executing any transfer, the originating VASP can cryptographically verify that the receiving address is owned by the intended legal entity.
3. **Man-in-the-Middle Attack Prevention:** Even if attackers compromise the API endpoint and substitute malicious addresses, the originating VASP will detect that the replacement address is not associated with the intended recipient's vLEI.



Technical Implementation Advantages

Preserved Protocol Compatibility:

VASPs can continue using existing IVMS and Travel Rule Protocol standards without disruption to current compliance workflows. The enhanced security layer operates transparently, requiring no changes to established processes while dramatically improving security.

Scalable Address Generation:

Receiving VASPs can generate new addresses for each transaction while maintaining vLEI verification, with all generated addresses organized as vLEI-verified smart contracts. This enables automatic verification regardless of address rotation policies, providing both security and operational flexibility.

Global Infrastructure Impact:

This capability becomes critical infrastructure for all exchanges and custodians globally, with universal adoption providing network-wide security benefits. Regulatory compliance is maintained while dramatically improving security, creating a foundation for enhanced trust across the entire cryptocurrency ecosystem.

Why Only vLEI Enables This Solution

The unique properties of vLEI credentials, built on KERI infrastructure, make this security enhancement possible as only vLEI provides the combination of cryptographic security through KERI in combination with legal entity verification backed by a high root of trust in GLEIF.

Autonomic identifier Features:

- ◆ **Pre-rotation:** Future keys are cryptographically committed, enabling seamless key updates
- ◆ **Lifelong Self-Certifying Identity:** Identifiers remain valid and verifiable indefinitely
- ◆ **Compromise Recovery:** Legitimate control can be restored even after key compromise
- ◆ **Compromise Detection:** Cryptographic mechanisms detect and prevent unauthorized key usage
- ◆ **Quantum Readiness:** Resistant to future quantum computing attacks

Hybrid Root of Trust:

- ◆ Combines cryptographic security with legal entity accountability
- ◆ GLEIF's foundational role provides global trust anchor
- ◆ Legal entity backing enables regulatory compliance and dispute resolution

Global Compatibility:

- ◆ Cryptocurrency operates inherently globally, requiring universal trust mechanisms
- ◆ vLEI provides the only globally recognized, cryptographically secure legal entity identification system
- ◆ No other solution combines the necessary technical security with legal entity verification

Implementation Benefits and Impact

Enhanced Security for All Participants

Originating VASPs receive cryptographic guarantees that funds are sent only to intended recipients, protection against sophisticated man-in-the-middle attacks, and maintained compliance with Travel Rule requirements. **Receiving VASPs** gain verifiable identity credentials that enhance trust with counterparties and provide competitive advantages through enhanced security posture, while reducing fraud risk. **For regulators**, the system enables improved compliance monitoring through verifiable audit trails, enhanced security that reduces systemic risk in the cryptocurrency ecosystem, and clear legal entity identification that supports enforcement actions.

Market-Wide Transformation

Universal Adoption Incentives:

- ◆ Security benefits create competitive pressure for vLEI adoption
- ◆ Network effects increase as more participants implement vLEI verification
- ◆ Regulatory preference for secure implementations drives market adoption

Infrastructure Resilience:

- ◆ Reduced attack surface for the entire cryptocurrency ecosystem
- ◆ Enhanced trust in institutional cryptocurrency services
- ◆ Foundation for additional compliance and security enhancements



5.4.4 Conclusion

The current Travel Rule implementations create a dangerous security vulnerability that threatens the entire cryptocurrency ecosystem. By mandating insecure communication protocols, regulators have inadvertently created a massive honeypot that sophisticated attackers will exploit to steal funds and harvest sensitive customer data.











Verifiable Smart Contracts provide the only viable solution to this security crisis. By enabling cryptographic verification of receiving addresses tied to verifiable legal entities, this approach maintains full Travel Rule compliance while eliminating the critical vulnerabilities in current implementations.

The unique properties of vLEI credentials—including autonomic identifiers, compromise recovery, and quantum readiness—make this security enhancement possible. Only vLEI provides the combination of cryptographic security and legal entity verification necessary to secure global cryptocurrency transactions while maintaining regulatory compliance.

This capability will become critical infrastructure for all exchanges and custodians globally, transforming the Travel Rule from a security liability into a foundation for enhanced trust and security in the cryptocurrency ecosystem.

5.5 Smart Contract Evolution

Institutional-Grade Capabilities: Traditional vs. Verifiable Smart Contracts

Enterprise Capability	Traditional Smart Contracts	Verifiable Smart Contracts
Legal Entity Identity Verification		
Compromise Recovery & Business Continuity		
Automated Regulatory Compliance		
Secure Travel Rule Implementation		
Cross-Chain Identity Portability		
Counterparty Verification & Risk Management		
Hierarchical Access Control		
Quantum-Resistant Security		
Institutional Fraud Prevention		

The Enterprise Differentiator: Traditional smart contracts lack institutional-grade security and compliance capabilities. Verifiable Smart Contracts bridge blockchain technology with enterprise requirements through cryptographically verified legal entity identity, enabling institutional adoption at scale.

06.

Which building blocks and infrastructure are needed?

The transformation to Verifiable Smart Contracts requires three critical infrastructure components to reach full maturity. **More vLEI Issuance & Infrastructure, Consensus on Standards used to tie ACDCs to contracts, Watchers and Oracles.** While some capabilities are already emerging, the complete vision outlined in this report depends on coordinated development across these key areas.

Web3s ISO 668 moment

ISO 668's standardization of shipping containers in 1968 revolutionized global trade by enabling seamless intermodal transport, slashing costs and dramatically increasing trade volumes worldwide. The web3 space is approaching its own ISO 668 moment as verifiable Legal Entity Identifiers (vLEI) emerge to standardize digital identity and therefore the transport of verifiable data across blockchain networks.



6.1 More Issuance and Infrastructure

The foundation of Verifiable Smart Contracts relies on widespread availability of vLEI credentials, which requires significant expansion of the current Qualified vLEI Issuer (QVI) ecosystem.

6.1.1 Currently Existing QVIs

The vLEI ecosystem currently operates with a limited number of Qualified vLEI Issuers globally:

- ◆ **United States:** One QVI serving the North American market
- ◆ **Asia:** One QVI based in Thailand
- ◆ **Europe:** One QVI providing European coverage
- ◆ **China:** Two QVIs serving the Chinese market
- ◆ **10+ more in the qualification** process at time of writing

This limited infrastructure creates bottlenecks for global adoption and maintains higher costs for vLEI credential issuance. However, turnkey solutions for onboarding new QVIs are already available, indicating that this infrastructure gap will likely be resolved in the near term and vLEI issuance pricing will trend down in perpetuity.^[23]

6.1.2 Enterprise-Grade User Interfaces and Platforms

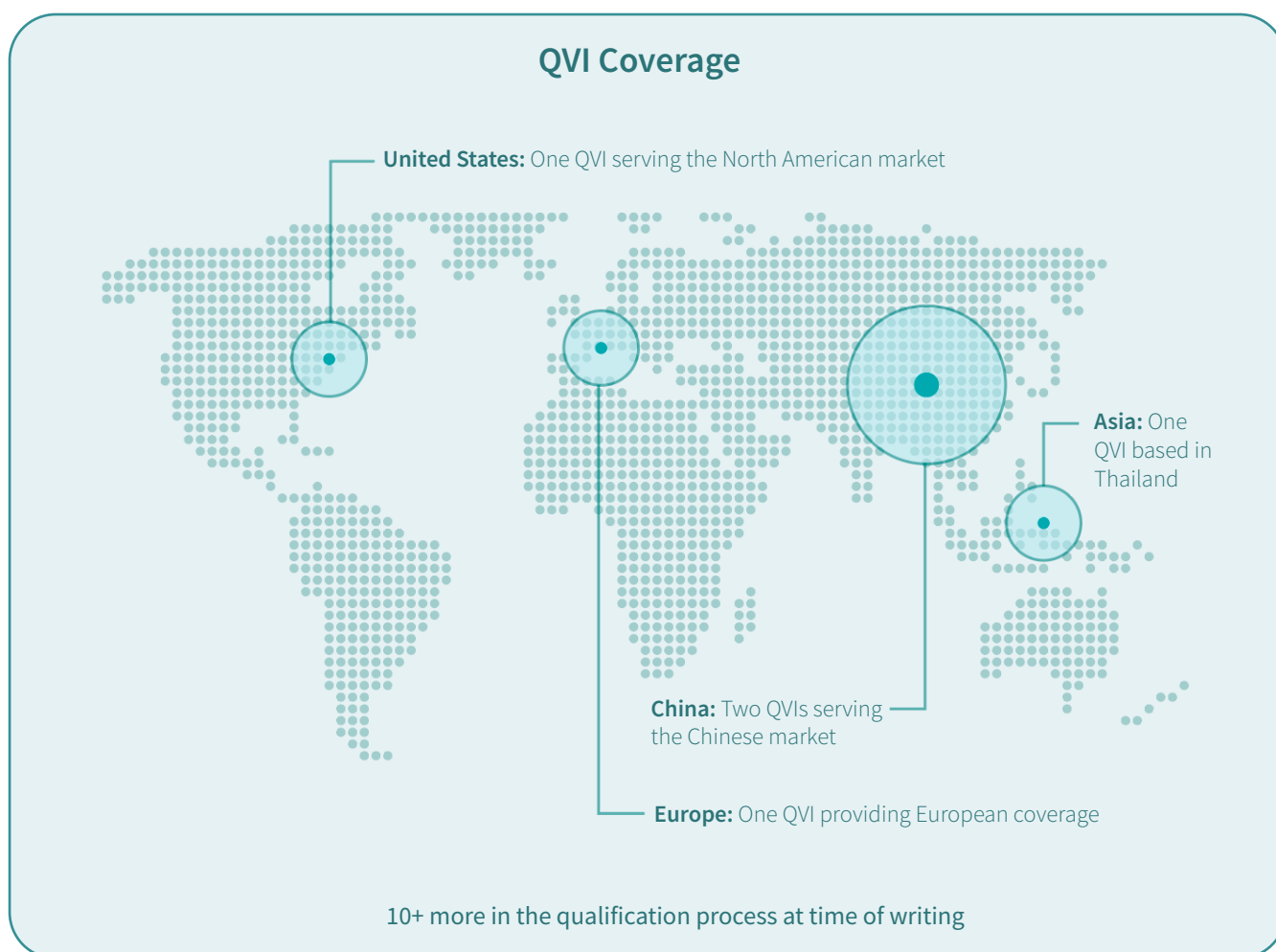
While vLEI management platforms exist, they have not yet been deployed at the scale necessary for mass enterprise adoption.^[23]

6.1.3 Crypto-Native Qualified vLEI Issuers

The most critical gap is the absence of crypto-native QVIs specifically designed to onboard the web3 ecosystem. Traditional QVIs focus primarily on conventional business use cases and lack the specialized knowledge, infrastructure, and user experience design necessary to serve blockchain-native organizations effectively.

6.1.4 Impact of Expanded Infrastructure:

As more QVIs come online globally, the price of vLEI credentials will trend downward significantly, making adoption at scale economically viable for smaller organizations and individual projects. This price reduction, combined with crypto-native onboarding processes, will accelerate adoption across the web3 ecosystem.



6.2. Consensus on Standards and Implementation

The second critical requirement is establishing industry consensus on how KERI ACDC credentials are tied to **Verifiable Smart Contracts**.

6.2.1 First-Mover Standard Setting

The first organization to successfully implement and deploy vLEI-enabled **Verifiable Smart Contracts** will effectively set the industry standard for how credentials are embedded, verified, and utilized within blockchain environments. This first-mover advantage carries significant responsibility, as their implementation choices will likely become the de facto standard across multiple blockchain ecosystems.

6.2.2 Cross-Chain Best Practices

Regardless of specific blockchain infrastructure, standardized best practices must emerge for:

- ◆ **Credential Embedding:** How ACDC credentials are incorporated into smart contract deployment or tied to them post-issuance
- ◆ **Interoperability Standards:** Ensuring **Verifiable Smart Contracts** function consistently across different blockchain networks
- ◆ **Security Frameworks:** Established best practices for secure credential management and key rotation

The development of these standards is imminent, with multiple players in the web3 community actively working toward implementation.

6.3. Global KERI Infrastructure: Watchers and Oracles

The final component required for full verifiable smart contract capability is the deployment of global KERI infrastructure, specifically “KERI watchers” and associated oracle networks.

6.3.1 The Role of Watchers in KERI

In the KERI ecosystem, watchers serve a critical function by monitoring Key Event Logs (KELs) of specific KERI autonomous identifiers on behalf of verifiers. A “superwatcher” or “global watcher” extends this concept by monitoring all KELs rather than watching specific identifiers on demand.

6.3.2 Oracle Integration Requirements

For smart contracts to perform on-chain verification of vLEI credentials, oracle networks must be able to:

- ◆ **Query Superwatchers:** Retrieve current key state information for any vLEI identifier
- ◆ **Verify Signatures:** Validate ACDC credentials against current key state
- ◆ **Provide Real-Time Data:** Deliver verification results to smart contracts with minimal latency

6.3.3 Implementation Timeline and Impact

Immediate capabilities (Available Soon):

Having expanded QVI infrastructure and consensus on credential embedding will enable:

- ◆ Off-chain verification of **Verifiable Smart Contracts**
- ◆ Enhanced fraud prevention through wallet-level verification
- ◆ Improved trust and transparency in token issuance
- ◆ Foundation for regulatory compliance frameworks

Full capabilities (Next Two Years):

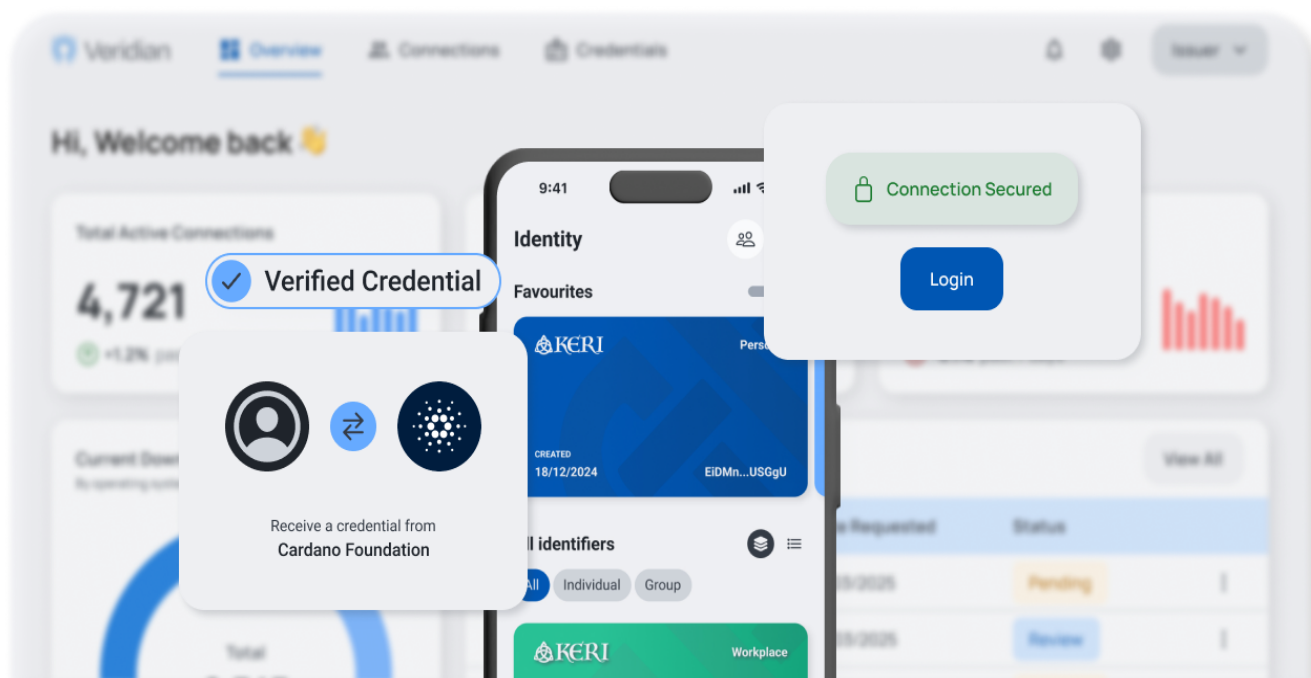
When required components are operational, they will enable:

- ◆ Complete on-chain verification of legal entity credentials
- ◆ Automated compliance checking within smart contracts
- ◆ True “money lego” functionality with verified counterparties
- ◆ Fundamental boost to on-chain security across all use cases
- ◆ All capabilities and use cases discussed throughout this report

Multiple players in the web3 community actively working toward implementation of the individual building blocks.^{[13][24][25][26]}

6.3.4 Early Movers: infrastructure and projects in development

Cardano



Veridian is the first KERI-based open source identity platform that anchors a tertiary root-of-trust on the Cardano blockchain.

The Cardano Foundation recognises the significance of a verifiable web3 supporting interoperability with traditional Web 2.0 and industry standards. Cardano's non-EVM blockchain offers security enhancements to smart contract developers and users by way of the EUTxO (Extended Unspent Transaction Output) model. **Cardano solves the challenges associated with EVM blockchain's account-based state management and non-deterministic smart contract execution.** In addition to Cardano's stateless and deterministic approach to transactions, native assets, and smart contracts, the Cardano Foundation recently launched the Veridian Platform.^[27]

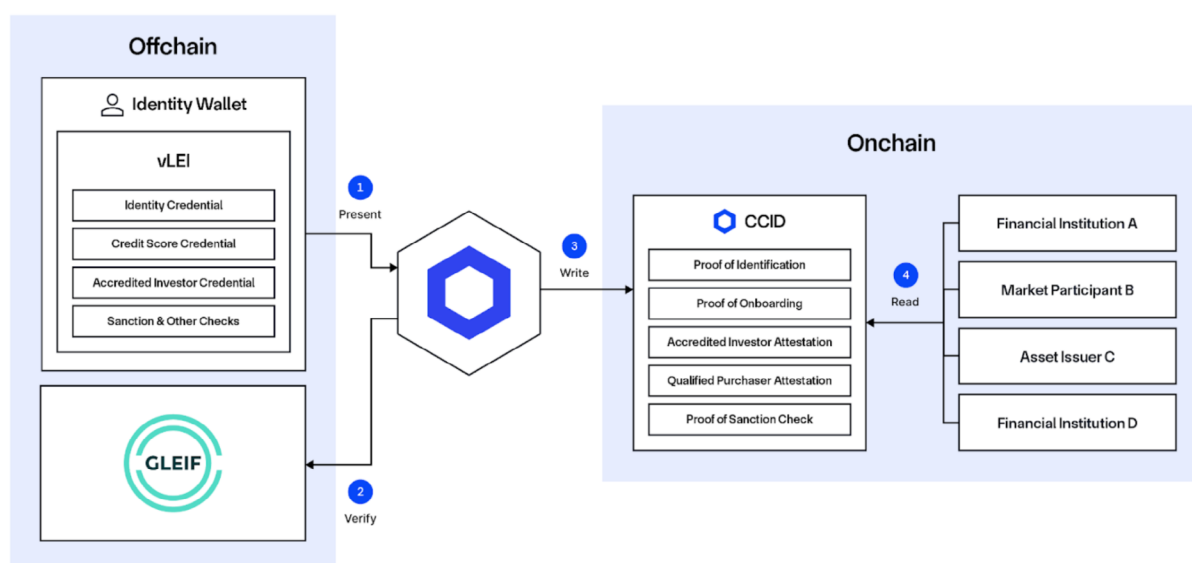
Veridian is the first KERI-based open source identity platform that anchors a tertiary root-of-trust on the Cardano blockchain. Veridian's approach to verifiable identity and blockchain support GDPR and related privacy regulations demonstrating a light-touch DLT approach to

decentralized identity. Furthermore, because Veridian is built atop the KERI protocol including the Trust Over IP's ACDC (Authentic Chained Data Container) specification, interoperability with GLEIF's vLEI technology within web3 can now be achieved.

The ability to anchor vLEI related proofs on-chain provides the fundamental building blocks for verifiable smart contracts and true interoperability beyond ecosystem boundaries including Web 2.0 and web3 networks. The Cardano Foundation team behind Veridian, Decentralized Trust and Identity Solutions, are also exploring the on-chain delegation of off-chain identifiers, verifiable native assets and how organizational identity can solve existing challenges within decentralized exchanges and finance.

[24] [27]

Chainlink



Chainlink's ACE & CCID: A Monumental Step Forward

In June 2025, Chainlink is announcing their Automated Compliance Engine (ACE) and Cross-Chain Identity (CCID) solution, representing what could be a step in the right direction toward **realizing the Verifiable Smart Contract vision outlined in this report.**

Chainlink contributed a statement on their upcoming products to this report. Their planned solution includes:

"Chainlink, the standard for on-chain finance, offers the Automated Compliance Engine (ACE)—a comprehensive suite of compliance-related capabilities, tools, and services connected with GLEIF's verifiable identity framework. Chainlink's Cross-Chain Identity (CCID) solution is being used to link on-chain wallets to the LEI/vLEIs of real-world legal entities, and includes accredited investor/qualified purchaser verification attributes through verifiable credentials issued by Virtual Asset Service Providers (VASP), financial institutions, Identity Verification (IDV) solutions, and more. This enables smart contracts, asset issuers, trading platforms, and asset administrators to verify that counterparties involved in a transaction have completed certain required identity checks and sanctions checks, supporting their onboarding of users to engage with their products.

Chainlink ACE provides institutions with the tools to unlock complex and compliant digital assets and financial transactions across multiple tokenized asset formats, jurisdictions, counterparties, and execution environments, including public and private blockchains, while also maintaining privacy of sensitive data. Now with the necessary standards and infrastructure to support compliance and preserve privacy, institutions can transition the world's capital to a blockchain-based format and create robust markets for tokenized assets."

At the time of writing, **Chainlink has not yet publicly released the technical specifications or implementation details for their ACE and CCID solutions.** While their announcement demonstrates a significant commitment to enabling vLEI integration with oracle infrastructure—potentially aligning with the Verifiable Smart Contract capabilities described in this report—we cannot confirm which specific use cases will be supported until implementation details are available.

To deliver the complete KERI and vLEI feature sets outlined in this report, two technical requirements are essential. First, users and observers must have access to ACDCs signed directly by the issuer, rather than cryptographic assertions in alternative formats from issuers who verified third-party ACDCs at an earlier time. Second, oracles need direct access to the KERI infrastructure associated with the Key Event Log (KEL) linked to a vLEI to maintain KERIs security features such as pre-rotation, quantum resilience and compromise detection.

This report will be updated as soon as more information on CCID and ACE is available.

6.4 The Race for Global Infrastructure

The development of global KERI watcher and oracle infrastructure represents a significant opportunity for first-movers in the blockchain infrastructure space. The organization or consortium that successfully deploys the first comprehensive KERI watcher-oracle network will play a foundational role in the verifiable smart contract ecosystem.

This infrastructure race is already underway, with multiple teams recognizing the transformative potential of KERI-enabled blockchain verification. The winner will not only capture significant economic value but will also help establish the technical standards that define how **Verifiable Smart Contracts** operate across the global blockchain ecosystem.

6.5 Conclusion

The infrastructure requirements for **Verifiable Smart Contracts** are well-defined and actively being developed. The combination of expanded QVI networks, standardized implementation practices, and global KERI infrastructure will transform blockchain technology from its current limitations into a truly enterprise-ready platform capable of supporting regulated financial activities at global scale.

The timeline for this transformation is measured in years, not decades, making this a critical moment for organizations to begin planning their verifiable smart contract strategies.

07.

Why now?

The Regulatory Imperative and Market Transformation

The convergence of regulatory acceleration and technological maturity has created a critical inflection point for blockchain adoption. As demonstrated throughout this report, **Verifiable Smart Contracts** powered by vLEI credentials **solve fundamental security and compliance challenges** that have constrained institutional blockchain adoption for over a decade.



7.1 The Knowledge Gap Creates Opportunity

The transformative potential of **Verifiable Smart Contracts** remains largely unknown to both regulators and the broader web3 community. This knowledge gap represents both an opportunity and an urgent call to action. Once capabilities such as compromise recovery, secure Travel Rule compliance, fraud prevention, and cryptographic address attribution become widely understood, the regulatory landscape will shift dramatically.

When regulators discover that smart contracts can be cryptographically bound to verified legal entities in a tamper-proof manner:

It would be grossly negligent not to expect—and ultimately mandate—this level of accountability for highly regulated institutions. The existence of compromise recovery mechanisms makes it equally reckless for regulators to permit critical financial infrastructure to operate without these safeguards.

7.2 Regulatory Momentum is Accelerating

Financial regulation is evolving at unprecedented speed, particularly as the United States ramps up its cryptocurrency oversight framework. New regulations are being written now, creating a narrow window to influence standards before they become entrenched. The time to communicate these capabilities is precisely now, as regulatory frameworks crystallize around current limitations rather than future possibilities.

7.3 The Paradigm Shift is Inevitable

Once these capabilities become known, the distinction between traditional smart contracts and Verifiable Smart Contracts will become fundamental to blockchain security architecture. Verifiable smart contracts offer demonstrably superior security, compliance, and accountability—making their adoption inevitable for any serious institutional use case.

The infrastructure enabling this transformation is not theoretical. Multiple players in the web3 community are actively developing these solutions. GLEIF provides the global root of trust through G20-mandated Legal Entity Identifiers. KERI infrastructure delivers the cryptographic foundations for autonomic identifiers with compromise recovery. **The standardization of vLEI-signed attestations in blockchain environments is imminent**, with first-movers poised to establish industry standards.^{[13][24][25][26]}

Crucially, this solution represents the most decentralized approach to achieving institutional-grade compliance and security. The KERI protocol enables every participant to run their own infrastructure without centralized points of failure or data silos. Unlike alternative compliance solutions that require centralized platforms or intermediaries, KERI's decentralized architecture allows organizations to maintain full control over their cryptographic infrastructure while participating in a global trust network. This is **the only way to stay true to the web3 ethos of decentralization and self-sovereignty** while simultaneously gaining the compliance and security capabilities outlined throughout this report.

7.4 A Call to Action

This report serves as both a high level technical roadmap and a regulatory wake-up call. **For web3 builders, the message is clear: begin implementing Verifiable Smart Contract standards now**, before regulatory mandates make them requirements rather than competitive advantages. **For regulators, the imperative is equally urgent: understand these capabilities before writing rules that assume their absence.**

The transformation from traditional to **Verifiable Smart Contracts** represents more than an incremental improvement—it fundamentally changes how we conceptualize security, trust, and accountability in decentralized systems. **This paradigm shift will redefine blockchain's role in global finance, making the technology finally ready for the institutional adoption that has long been promised but never delivered.**

The question is not whether this transformation will occur, but whether stakeholders will lead it or be forced to follow it. There is a window of opportunity, while the standards are still being written and the competitive advantages are still available to early adopters.

For web3 builders, the message is clear: begin implementing verifiable smart contract standards now, before regulatory mandates make them requirements rather than competitive advantages.

For regulators, the imperative is equally urgent: understand these capabilities before writing rules that assume their absence.

08.

Conclusion

Verifiable Smart Contracts represent the missing link between blockchain technology's promise and its institutional reality. By solving the fundamental identity and trust challenges that have constrained blockchain adoption, **Verifiable Smart Contracts will unlock the full potential of decentralized finance while meeting the highest standards of regulatory compliance and security.**

The convergence of GLEIF's global trust infrastructure, KERI's breakthrough cryptographic capabilities, and accelerating regulatory frameworks has created a unique moment in blockchain history. **Those who recognize and act on this opportunity will shape the future of digital finance. Those who ignore it will find themselves operating with obsolete technology in an increasingly regulated world.**

The era of Verifiable Smart Contracts is beginning. The only question is who will lead the transformation. ■

9. Sources

- [1] DefiLlama [Internet]. [cited 2025 Jun 5]. Available from: <https://defillama.com/hacks>
- [2] Struckman K, Binder M. The Bybit Heist: What Happened & What Now? [Internet]. 2025 [cited 2025 Jun 5]. Available from: <https://www.wilsoncenter.org/article/bybit-heist-what-happened-what-now>
- [3] 2024 WazirX hack. In: Wikipedia [Internet]. [cited 2025 Jun 5]. Available from: https://en.wikipedia.org/wiki/2024_WazirX_hack
- [4] Warren-Kachelein D. Crypto Hackers Exploit Ronin Network for \$615 Million [Internet]. 2022 [cited 2025 Jun 5]. Available from: <https://www.bankinfosecurity.com/crypto-hackers-exploit-ronin-network-for-615-million-a-18810>
- [5] Radiant Capital. Radiant Capital Post-Mortem [Internet]. 2024 [cited 2025 Jun 5]. Available from: <https://medium.com/@RadiantCapital/radiant-post-mortem-fecd6cd38081>
- [6] GLEIF. Get an LEI: Find LEI Issuing Organizations [Internet]. [cited 2025 Jun 5]. Available from: <https://www.gleif.org/en/organizational-identity/get-an-lei-find-lei-issuing-organizations/>
- [7] GLEIF. LEI Search [Internet]. [cited 2025 Jun 5]. Available from: <https://search.gleif.org/#/search/simpleSearch=>
- [8] Unique Transaction Identifier. In: Wikipedia [Internet]. 2024 [cited 2025 Jun 5]. Available from: https://en.wikipedia.org/w/index.php?title=Unique_Transaction_Identifier&oldid=1200457019
- [9] Grody A. CFTC Continues to Lead - Stepping Up to Global Data Mandates [Internet]. 2020 [cited 2025 Jun 5]. Available from: <https://derivsource.com/2020/04/01/cftc-continues-to-lead-stepping-up-to-global-data-mandates/>
- [10] GLEIF. The vLEI: Introducing Digital I.D. for Organizations Everywhere [Internet]. [cited 2025 Jun 5]. Available from: <https://www.gleif.org/en/organizational-identity/introducing-the-verifiable-lei-vlei/gleif-ebook-the-vlei-introducing-digital-i-d-for-organizations-everywhere>
- [11] Key State Capital. vLEI The Rise of Organizational Digital Identity [Internet]. 2025 April [cited 2025 Jun 5]. Available from: <https://assets.keystate.capital/vLEI%20-%20The%20Rise%20of%20Organizational%20Digital%20Identity.pdf>
- [12] Smith SM. KEY EVENT RECEIPT INFRASTRUCTURE (KERI) DESIGN [Internet]. 2019 Mar 7 [cited 2025 Jun 5]. Available from: https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf
- [13] Dow H. GuildOne introduces decentralized identity trust layer for R3 Corda/Cardano climate interoperability [Internet]. GuildOne; 2024 [cited 2025 Jun 9]. Available from: <https://guild1.co/guildone-introduces-decentralized-identity-trust-layer-for-r3-corda-cardano-climate-interoperability/>
- [14] Chainlink. Beyond Token Issuance [Internet]. 2024 Apr [cited 2025 Jun 5]. Available from: <https://pages.chain.link/hubfs/e/definitive-guide-to-tokenized-assets.pdf>
- [15] Hamilton M. 9 Barriers to the Tokenization of Real World Assets - Crypto Blockchain Lawyer [Internet]. Hamilton and Associates; 2024 [cited 2025 Jun 5]. Available from: <https://law-kc.com/articles/9-barriers-to-the-tokenization-of-real-world-assets>
- [16] Decentralized Finance is Booming — So Are the Security Risks [Internet]. 2025 [cited 2025 Jun 5]. Available from: <https://research.gatech.edu/decentralized-finance-booming-so-are-security-risks>
- [17] imToken - Ethereum Wallet, Bitcoin Wallet - Help Center [Internet]. 2024 [cited 2025 Jun 12]. Be wary of the fake transaction record scam! Available from: <https://support.token.im/hc/en-us/articles/17009391596697-Be-wary-of-the-fake-transaction-record-scam>
- [18] FATF. Targeted Update on Implementation of the FATF Standards on VAs and VASPs [Internet]. Paris, France: Financial Action Task Force; 2024 Jun [cited 2025 Jun 5]. Available from: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>
- [19] Notabene. Crypto Travel Rule Regulations in European Union by EU Parl [Internet]. 2024 [cited 2025 Jun 5]. . Available from: <https://notabene.id/world/eu>
- [20] interVASP Messaging Standard 101 (IVMS 101) [Internet]. [cited 2025 Jun 5]. Available from: <https://www.intervasp.org/>
- [21] OpenVASP Association [Internet]. [cited 2025 Jun 5]. Available from: <https://www.openvasp.org/trp>
- [22] Betschart L. How the TRP Travel Address Solves the FATF Travel Rule [Internet]. [cited 2025 Jun 5]. Available from: <https://www.21analytics.ch/blog/how-the-trp-travel-address-solves-the-fatf-travel-rule/>
- [23] Provenant. Streamlining vLEI Onboarding | Secure Regulatory Compliance for Banks [Internet]. [cited 2025 Jun 5]. Available from: <https://www.vlei.finance/>
- [24] Mayfield TA. Veridian represents the future of digital identity management for individuals and enterprises [Internet]. Cardano Foundation; [cited 2025 Jun 5]. Available from: <https://cardanofoundation.org/blog/veridian-digital-identity-platform>
- [25] Chainlink. Sibos 2024: Connecting the Future of Finance Onchain [Internet]. Chainlink Blog; 2024 [cited 2025 Jun 5]. Available from: <https://blog.chain.link/sibos-2024-recap/>
- [26] GLEIF, Chainlink. The Future of Digital Identity and Automated Compliance in Global Financial Services [Internet]. 2025 Jun [cited 2025 Jun 5]. Available from: https://pages.chain.link/hubfs/e/GLEIF_Chainlink_Identity_Report.pdf
- [27] Veridian Platform Website [Internet]. [cited 2025 Jun 12]. Available from: <https://www.veridian.id/>
- [28] Chainlink. Sibos 2024: Connecting the Future of Finance Onchain | Highlights [Internet]. Chainlink Blog. 2024 [cited 2025 Jun 12]. Available from: <https://blog.chain.link/sibos-2024-recap/>
- [29] International Organization of Securities Commissions. Policy recommendations for decentralized finance (DeFi): Final report. 2023 [cited 2025 Jun 16]. Available from: <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD754.pdf>
- [30] Chainalysis Team. \$2.2 billion stolen from crypto platforms in 2024, but hacked volumes stagnate toward year-end as DPRK slows activity post-July [Internet]. 2024 [cited 2025 Jun 16]. Available from: <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>

Contact or questions:
contact@keystate.capital

