BLOCKCHAIN IDENTITY REPORT

The Future of Digital Identity and Automated Compliance in Global Financial Services

June 2025

GLEIF

Chainlink

Foreword

Identity verification processes are a crucial component of maintaining regulatory compliance in global financial services, serving as a foundational defense against fraud, money laundering, terrorist financing, sanctions violations, and other illicit financial activities. However, existing identity verification frameworks often rely on manual and fragmented approaches, which are duplicated within each firm due to stringent data protection requirements, differences in policies, and a lack of standardization. This results in significant operational inefficiencies, high compliance costs, and customer friction—while still leaving institutions vulnerable to sophisticated financial crimes.

According to a 2024 KYC (Know-Your-Customer) survey by Fenergo, financial institutions in the UK, U.S., and Singapore spend roughly 33% of their compliance budgets on KYC alone.[1] On average, global financial institutions have 1,566 employees involved in the AML/KYC process, resulting in an average cost of $2,598 per client onboarding.[2] Compounding these costs, Fenergo estimates these slow and inefficient onboarding processes have led to 67% of banks and 74% of asset managers losing clients.[3]

Despite these costly efforts, financial institutions still faced $4.6 billion in fines for failing to meet AML and KYC obligations in 2024.[4] These penalties are often accompanied by lasting reputational damage and loss of client trust—making digital identity not just a compliance issue, but a strategic priority.

High-profile failures and resulting regulatory responses mean that financial institutions must navigate increasingly stringent and costly KYC, Anti-Money Laundering (AML), and sanctions screening requirements to combat fraud and illicit finance. Despite stricter customer onboarding processes, the scale of financial crime is an ongoing concern. According to a Nasdaq financial crime report, an estimated $3.1 trillion in illicit funds flowed through the global financial system in 2023.[5] Scams and bank fraud schemes contributed to approximately $485.6 billion in losses globally.

Data protection regulations, such as the EU's General Data Protection Regulation (GDPR), impose additional challenges. While firms are required to conduct extensive due diligence on their clients and customers, handling and storing personally identifiable information (PII) comes with substantial regulatory obligations. These include stringent data management requirements, such as ensuring data sovereignty, preventing unauthorized data transfers outside the EU, and maintaining compliance with data retention and privacy rights. As a result, firms are wary of managing customer data internally.

Financial markets and services are also evolving to include tokenized assets and decentralized finance (DeFi), enabling the end-to-end automation of financial services at scale. This shift makes secure, verifiable, and highly efficient identity processes more critical than ever—especially for organizations.

Addressing the core inefficiencies present in today's identity verification processes requires moving from a fragmented model—where verification processes are independently and repeatedly duplicated within each individual institution—to a more efficient, interoperable, blockchain-based model where identity verifications can be securely accessed and shared between multiple entities. Building upon the established ISO 17442 Legal Entity Identifier (LEI), the verifiable LEI (vLEI) can help institutions make this move successfully.

Blockchain-based digital identity offers a different approach that saves time and costs while enhancing privacy and security. Instead of validating and storing customer data in-house, organizations can use cryptographic proofs, which can verify that a user meets key identity requirements without exposing their private information. These proofs can then be tied to digital identities onchain. Combined with vLEIs, organizations can have certainty around the identity of a counterparty and share relevant identity attributes on a need-to-know basis when transacting onchain, all while maintaining the ability to enforce their own policies and protect user privacy when using shared identity data.

[1] Fenergo: KYC in 2024
[2] J.P. Morgan: Project EPIC
[3] Fenergo: KYC Trends
[4] Fenergo: AML Enforcement Action in 2024
[5] Nasdaq: Global Financial Crime Report

If implemented correctly, blockchain-based identity reduces the need to verify the same data repeatedly across different institutions. This helps reduce compliance headaches, minimizes data exposure, and enables faster onboarding without sacrificing regulatory integrity, provided the implementation aligns with data protection rules.

While blockchain technology can improve identity verification processes for global financial markets, it's critical that financial institutions have a shared standard to connect blockchain-based identity with existing infrastructure and regulatory frameworks. This report, produced by the Global Legal Entity Identifier Foundation (GLEIF) and Chainlink, explores how such a standard can be applied across financial services.

GLEIF's work on global digital organizational identity and Chainlink's blockchain infrastructure both support identity systems that are secure, work across different platforms, and easily connect with existing systems. GLEIF's vLEI enables organizations to prove their identity off and onchain, while Chainlink enables firms to verify identity without exposing sensitive information and make identity portable across multiple chains and legacy systems.

This report explores these standards and makes the case for blockchain-enabled identity in global financial services.

Part 1: Digital Identity Verification in Financial Services Today

Identity verification is the first line of defense against financial crime. Whether onboarding a new institutional client, executing trades, or transferring funds, firms must know exactly who they're dealing with to prevent fraud and money laundering on their platforms. Strict identity checks help keep fraudsters and sanctioned entities at bay.

> **"Financial fraud has increased and diversified significantly, both in terms of the volume of fraud offences and the methods deployed to perpetrate them. Today, financial fraud represents a pervasive, global threat."**
>
> Interpol: Global Financial Fraud Assessment, March 2024.[6]

Confirming identities also builds trust in financial transactions. It reduces the risk of fraud, chargebacks, and regulatory breaches—making it safer and more reliable to do business with verified organizations. At a broader level, effective identity checks help maintain integrity in global financial services.

[6] Interpol: INTERPOL Financial Fraud assessment: A global threat boosted by technology

Navigating the conflict between AML/KYC requirements and data privacy regulations

Increasingly strict global identity regulations are a requirement for financial firms today. The table below lists some of the many regulations that global financial institutions may need to consider:

Country / Region	Regulation	Brief summary of requirements
United States	Bank Secrecy Act (BSA) & USA PATRIOT Act	KYC, Customer Identification Programs (CIP), and Suspicious Activity Reporting (SAR).
European Union	AMLD4 & AMLD5	Customer due diligence, transaction monitoring, and crypto AML rules.
United Kingdom	Money Laundering Regulations 2017	Aligns with EU rules. Identity checks, risk-based monitoring, and record-keeping.
Singapore	CDSA & MAS AML Guidelines	Perform KYC, report suspicious transactions, and prevent illicit finance.
Japan	Act on Prevention of Transfer of Criminal Proceeds	Customer due diligence and transaction reporting for financial institutions.
India	Prevention of Money Laundering Act (PMLA)	Perform KYC and maintain financial records.
Canada	Proceeds of Crime (PCMLTFA)	Report large transactions, verify clients, and monitor suspicious activity.
Australia	AML/CTF Act 2006	Customer identity verification, transaction reporting, and ongoing compliance.

While these regulations strengthen market stability and integrity, they also create major compliance costs for organizations. In the UK, for example, firms spend an average of £21,000 per hour meeting regulatory obligations, according to a 2024 report by LexisNexis Risk Solutions.[7] In North America, financial institutions spent a combined $61 billion on financial crime compliance in 2023—up from approximately $50 billion in 2021—based on a separate study by LexisNexis.[8]

On the other side of the regulatory equation, firms must also comply with strict data protection laws. They're required to verify customer identities, monitor transactions, and report suspicious activity—all while minimizing data collection and protecting personal information. **This creates a fundamental conflict: firms are expected to collect and store sensitive identity data while also limiting their use of it.**

> **"At the moment, tectonic plates of data privacy and AML efforts clash in many parts of the world with not enough being done to improve on anonymisation via Privacy Enhancing Technologies and sharing of information."**
>
> KPMG, Financial Crime, a Paradigm Shift.[9]

[7] LexisNexis Risk Solutions: The True Costs of Compliance
[8] PR Newswire: Study Reveals Annual Cost of Financial Crime Compliance Totals $61 Billion in the United States and Canada
[9] KPMG: Financial Crime, a Paradigm Shift

Key data protection regulations that financial firms must navigate alongside AML/KYC requirements include:

Country / Region	Regulation	Brief summary of requirements
United States	California Consumer Privacy Act (CCPA)	Grants consumers the right to access, delete, and restrict sharing of their personal data.
European Union	General Data Protection Regulation (GDPR)	Limits data collection, requires user consent, and mandates strict data storage and deletion policies.
United Kingdom	UK GDPR & Data Protection Act 2018	Mirrors EU GDPR.
Singapore	Personal Data Protection Act (PDPA)	Consent for data collection, limits data use, and requires secure storage of personal information.
Japan	Act on the Protection of Personal Information (APPI)	Strict rules for data collection, sharing, and storage.
India	Digital Personal Data Protection Act 2023 (DPDP Act)	Requirements for handling personal data, including user consent.
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Gain consent before collecting personal data, protect stored data, and allow individuals to collect and correct their information.
Australia	Privacy Act 1988 & Consumer Data Right (CDR)	Limits the use of personal data, grants consumers control over their financial data, and has strict cyber security standards.

Streamlining identity verification across the financial system

Identity verification in financial services is often fragmented and delayed. Even when the same institutional client is known to multiple parties in a transaction, each regulated firm must verify that client's identity independently.

In response, the industry adopted Swift's KYC Registry, which allows financial institutions to upload standardized identity information in a secure environment. Other participating institutions can then access that information to streamline their own KYC checks—without having to request and validate identity data from scratch.

This setup improves efficiency across traditional financial services. However, it doesn't yet solve the emerging need for identity verification across blockchains.

Example workflow: Identity verification using Swift's KYC registry

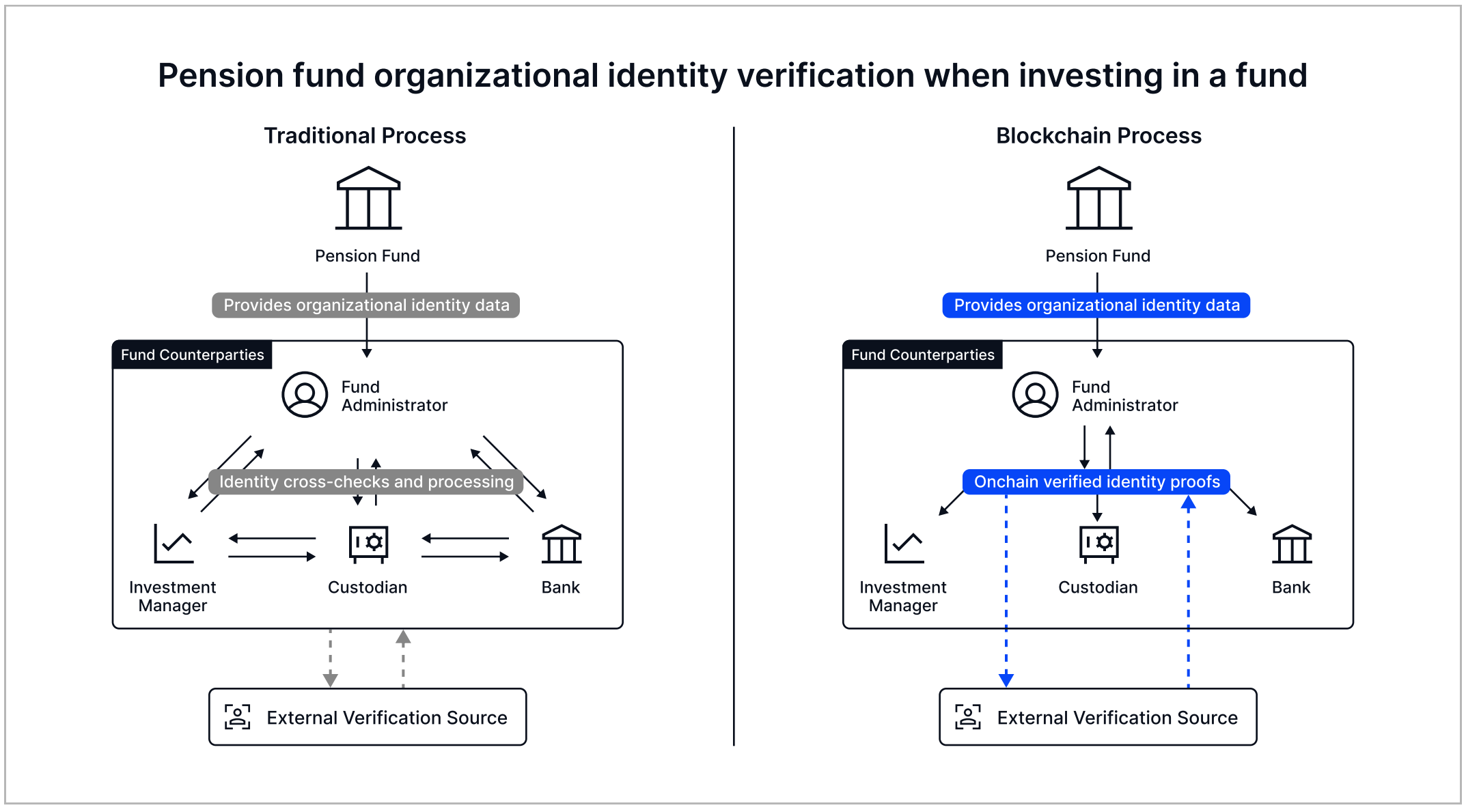
Part 2: The Opportunity of Blockchain-Enabled Identity in Financial Services

Traditional identity verification relies on centralized databases, where each institution runs its own checks, stores client data separately, and must repeatedly verify information—often manually. This creates duplication, high costs, and added compliance risks.

With blockchain-enabled identity, private identity information remains offchain while verifications of the data are stored onchain, where they're tied to a digital identity. Institutions can then access and request identity proofs—attestations stored on a blockchain that verify identity attributes have been validated by a trusted party—to the extent required for their own verification processes, without needing to store identity data internally. Assuming the identity proofs are accurately generated and securely stored onchain, this approach has several advantages over traditional identity verification methods:

- **Faster onboarding:** Verify identity instantly from a trusted source instead of repeating manual checks.
- L**ower compliance costs:** Reduce manual checks and duplicated processes. This streamlines regulatory reporting and cuts down operational expenses.
- **Eliminate data vulnerabilities:** No need to store sensitive identity data in multiple databases, reducing the possibility of data breaches.
- **Regulatory alignment:** Verify identity while accessing only the data needed. This balances AML, KYC, and sanctions screening requirements with data privacy regulations.
- **Automated compliance:** Once identity is verified, smart contracts can continuously enforce compliance rules without manual intervention. This ensures real-time adherence to AML, KYC, and reporting requirements, reducing delays, errors, and the need for repetitive compliance reviews.

Example workflow for verification of an institutional fund client: The diagram below contrasts the difference between a typical traditional process and a blockchain process for onboarding an institutional fund client (e.g., a pension fund). In both cases, the client would typically submit identity data to the fund administrator—but the key differences lie in what comes next.



In the **traditional process**, stakeholders cross-check and validate the pension fund's data among themselves or through siloed systems. This back-and-forth communication can not only be time-consuming and expensive, but may also result in data being overlooked or misinterpreted.

In the **blockchain process**, the fund administrator submits the pension fund's organizational identity proofs onto a distributed ledger for onchain validation and storage. Now, each stakeholder can pull the relevant identity proofs from a single source. Given the security design of blockchains, stakeholders have a clear audit trail.

Regulatory authorities and third-party KYC providers also interact with the blockchain. Instead of financial institutions submitting this compliance data separately, it flows directly into the blockchain. This means that when stakeholders retrieve identity proofs, they're also accessing the most up-to-date compliance status in real time. By feeding verified regulatory data into the blockchain, these sources help ensure that institutions are always working with accurate, tamper-proof information. This approach also vastly reduces manual work for firms.

What do regulators and market participants think about blockchain-enabled identity currently?

Regulators see the potential of blockchain for identity verification but highlight concerns around privacy, data protection, and standardization. The lack of global regulatory frameworks also makes compliance complex.

For example, a 2024 paper by the International Association for Trusted Blockchain Applications (INATBA) highlights how blockchain's immutability conflicts with GDPR's "right to be forgotten" rule.[10] Decentralized systems also make it hard to assign accountability, as there's no single entity responsible for controlling or maintaining the data.

That said, privacy-preserving tools like Chainlink's DECO generate cryptographic proofs offchain without exposing personal data. These proofs can be submitted onchain if needed, enabling verification without compromising privacy—which may help address some GDPR concerns.

Meanwhile, a recent J.P. Morgan report argues that solving digital identity is the key to scaling blockchain-based finance:

> **"Privacy-preserving, reusable digital identity solutions are fundamental to unlocking tokenization's full potential, enabling streamlined onboarding, real-time verification, and programmable compliance."**
>
> Kinexys by J.P. Morgan.[11]

The European Union is also advancing blockchain-based identity through the European Blockchain Services Infrastructure (EBSI).[12] Among other things, this initiative aims to support digital identity to help streamline compliance and build trust in digital identity systems.

[10] INATBA: INATBA Publishes Position Paper on Leveraging ZKPs for GDPR Compliance
[11] J.P. Morgan: Project Epic Whitepaper
[12] European Commission: European Blockchain Services Infrastructure

> “One day, I expect tokenized funds will become as familiar to investors as ETFs — provided we crack one critical problem: identity verification.
>
> Financial transactions demand rigorous identity checks. Apple Pay and credit cards handle identity verification effortlessly, billions of times a day. Trade venues like NYSE and MarketAxess manage to do the same for buying and selling securities. But tokenized assets won’t run through those traditional channels, meaning we need a new digital identity verification system.
>
> The takeaway is clear. If we're serious about building an efficient and accessible financial system, championing tokenization alone won't suffice. We must solve digital verification, too.”
>
> BlackRock CEO Larry Fink’s 2025 Annual Chairman’s Letter to Investors.[14]

Part 3: GLEIF and Chainlink’s Role in Organizational Identity and Automated Compliance

Before 2008, legal entity identity verification existed, but mostly at a national level. Each country had its own system for identifying businesses and individuals, and financial firms relied on proprietary internal databases to track counterparties. There was no global standard for identity verification, which made it difficult to assess risk exposure across jurisdictions.

The Lehman Brothers collapse fully exposed this issue. Lehman included multiple legal entities, and many external institutions had exposure to them. But when those legal entities failed, external counterparties had no way to quickly understand their exposure. Moreover, regulators had no way to gauge the broader situation. The fragmented identity systems made it nearly impossible to map the interconnectedness of financial firms in real time.

In response, leaders from the world’s largest economies, operating through the G20 and the Financial Stability Board, agreed to develop the Legal Entity Identifier (LEI), a standardized and universal means of identifying legal entities engaged in financial transactions and other official interactions. The LEI is a 20-digit alpha-numeric code, defined by ISO 17442, that connects to a verified business registration and information record held in the Global LEI Index, a data bank maintained by the Global Legal Entity Identifier Foundation (GLEIF) and made available to everyone, everywhere, free of charge. As of Q1 2025, there are over 2.71 million active LEIs globally.[15]

[14] BlackRock: Larry Fink’s 2025 Annual Chairman’s Letter to Investors

From LEIs to vLEIs: Bringing organizational identity onchain

LEIs may have brought global standardization to organizational identity in financial markets, but much of the verification process still relies on external lookups and manual checks. KYC and identity checks for individuals—such as high-net-worth clients in banking and wealth management—also face similar challenges. Data privacy regulations like GDPR further complicate how firms handle personally identifiable information (PII) while complying with AML and KYC requirements.

But as markets have become increasingly digital and decentralized, a new challenge has emerged: integrating legal identity systems into blockchain-based finance. This shift includes decentralized finance (DeFi), tokenized assets, and cross-chain transactions—which all need digitally verifiable organizational identity.

GLEIF's vLEI is a cryptographic secure digital counterpart of a conventional LEI. In other words, it is a digitally trustworthy version of the 20-digit LEI code which is automatically verified, without the need for human intervention. It gives government organizations, companies, and other legal entities worldwide the capacity to use non-repudiable identification data pertaining to their legal status ownership structure and authorized representatives in any kind of digital interaction, transaction or e-signature scenario.

When the vLEI is combined with Chainlink's infrastructure, it can bring hierarchical trust into the digital world. First, a legal entity obtains a traditional LEI—establishing its legitimacy. An organization accredited as a Qualified vLEI Issuer can then issue vLEI credentials to the entity, enabling the entity to issue downstream identity credentials to sub-entities and employees, such as a corporation, regional branch, and risk officer. This extends trust from an organization to its subsidiaries and representatives. For example, a regional CFO can sign a transaction with their vLEI role credentials, verifying they have the authority to approve a transaction within a certain jurisdiction and enabling it to then be processed automatically. Entities can also issue credentials to parties they are engaged with, for example, a bank can issue a verifiable credential to an institutional or retail client attesting that the client has completed KYC verification.

These credentials are cryptographically secure and automatically verifiable in real time. Chainlink's infrastructure allows these vLEIs to be used seamlessly and securely across the blockchain ecosystem, enabling trusted access and identity-based permissions in DeFi and other onchain applications. Ultimately, this enables institutions to move financial services onchain while continuing to meet high regulatory standards.

While vLEIs provide a standardized way to prove an organization's identity, they're only part of the broader movement toward decentralized digital identity. GLEIF supports an open ecosystem where any qualified issuer can adopt the vLEI standard and help build a shared trust framework. The vLEI ecosystem is still developing and continues to grow with each new partnership. GLEIF doesn't issue all credentials directly. Instead, it acts as the root-of-trust for all vLEIs, and enables qualified third-party issuers to offer organizational identity via the vLEI standard—creating an open, scalable model for trust across financial services.

[15] Global Legal Entity Identifier Foundation (GLEIF): Global LEI Index Statistics

Enabling secure cross-chain interoperability while preserving user privacy

For vLEIs and blockchain identity solutions to work at scale, they need privacy, interoperability, and offchain integration. That's where Chainlink's infrastructure plays a critical role:

Chainlink Blockchain Privacy Manager: The Blockchain Privacy Manager enforces fine-grained access policies and redacts sensitive information at the infrastructure level, ensuring only authorized identity proofs are shared. This allows smart contracts on public or private chains to verify organizational credentials, such as vLEIs, without exposing underlying personal or entity data. CCIP Private Transactions extends this by enabling encrypted cross-chain messaging, allowing identity verifications to occur confidentially across separate blockchains.

Chainlink DECO: DECO provides an advanced privacy-preserving data verification system, which uses zero-knowledge proofs (ZKPs) and existing web infrastructure to enable financial institutions, enterprises, and Web3 developers to verify sensitive identity information across blockchains without exposing the underlying data.

Chainlink Cross-Chain Interoperability Protocol (CCIP): Chainlink CCIP enables developers to build secure applications that can transfer tokens, send messages, and initiate actions across blockchains, and connect with legacy systems

CCIP is built with defense-in-depth security and is the only interoperability protocol with level-5 cross-chain security and features additional layers of protection via the Risk Management Network and transfer rate limits. Chainlink CCIP and its first-of-its-kind Risk Management Network is the only infrastructure capable of supporting a secure and scalable cross-chain economy for both DeFi and traditional finance.

To gain more insights into how GLEIF and Chainlink are supporting secure digital identity solutions, watch this discussion between Chainlink Co-Founder Sergey Nazarov and GLEIF CEO Alexandre Kech at Sibos.

Looking ahead: Increasing trust and integrity of global markets

Since 2008, the introduction of global identity standards has significantly increased the integrity of financial markets. However, today's identity systems remain highly fragmented, imposing high costs, slowing onboarding, and creating friction between regulatory compliance and data protection. Verifiable onchain identity is essential to the future of global financial services as the adoption of digital assets continues to grow.

GLEIF and Chainlink can solve this challenge by bringing globally recognized and regulatory overseen identity standards into the blockchain era. GLEIF's vLEIs offer a cryptographically secure, standardized way to prove an organization's identity onchain, while Chainlink provides the infrastructure to support secure interoperability across multiple blockchains and existing financial systems, while protecting user privacy. As part of a rapidly growing ecosystem onchain, these standards are set to increase the trust and integrity of financial markets globally.

About GLEIF

Established by the Financial Stability Board in June 2014, the Global Legal Entity Identifier Foundation (GLEIF) is a not-for-profit organization created to support the implementation and use of the Legal Entity Identifier (LEI) and its digital counterpart the verifiable LEI (vLEI). GLEIF is headquartered in Basel, Switzerland.

GLEIF's mission is to manage a network of global partners to provide trusted services and open, reliable data for unique legal entity identification worldwide. GLEIF makes available the technical infrastructure to provide, via an open data license, online access to the full global LEI database free of charge to users. GLEIF is overseen by the Regulatory Oversight Committee, which is made up of representatives of public authorities from across the globe.

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

For more information, visit the GLEIF website at gleif.org.

Source:

Global Legal Entity Identifier Foundation, St. Alban-Vorstadt 12, 4052 Basel, Switzerland
Chair of the Board: Teresa Glasser, CEO: Alexandre Kech
Commercial-Register-No.: CHE-200.595.965, VAT-No.: CHE-200.595.965MWST

LEI: 506700GE1G29325QX363

About Chainlink

Chainlink is the standard for onchain finance, verifiable data, and cross-chain interoperability. Chainlink is unifying liquidity across global markets and has enabled over $20 trillion in transaction value across the blockchain economy. Major financial market infrastructures and institutions, such as Swift, Fidelity International, and ANZ Bank, as well as top DeFi protocols including Aave, GMX, and Lido, use Chainlink to power next-generation applications for banking, asset management, and other major sectors. Learn more by visiting chain.link.

If you're interested in accelerating your digital assets strategy, reach out to our team.

CONTRIBUTORS

GLEIF

Alexandre Kech
CEO

Chainlink

Angie Walker
Global Head of Capital Markets