AN ACCENTURE X CHAINLINK RESEARCH COLLABORATION

Liquidity Without Borders

Why Cross-Chain Interoperability Is Essential in an Increasingly Multi-Chain Financial Services Landscape

accenture

IN COLLABORATION WITH

Chainlink

May 2025

Introduction

Financial services firms have intensified their adoption of blockchains, distributed ledger technology (DLT), and programmable ledgers (collectively referred to as "distributed ledgers"[1]). Central to this acceleration in adoption is tokenization, the process of recording ownership of, or natively issuing, a financial asset to be traded, owned, and managed on a distributed ledger. Tokenization promises a range of advantages—enhanced liquidity, streamlined workflows, reduced settlement risk, increased programmability, and broader accessibility—that stand to transform financial markets.

Despite this promise, the adoption of distributed ledgers by financial services entities[2] has largely occurred in silos because of various market forces, such as data privacy concerns and competitive elements, **giving rise to "digital liquidity islands"**[3]. If left unchecked, this trend could hinder onchain financial products as access to investors, capital and other financial services can be limited. As the industry develops more public, public-permissioned, and private distributed ledgers[4], the question of cross-chain interoperability is elevated, However the privacy concerns that have hampered adoption of public distributed ledgers by regulated entities are increasingly being addressed by sophisticated security and compliance solutions.

The industry is at a tipping point where deep collaboration will allow the activation of a multi-trillion-dollar transformation. To illuminate the opportunity, Accenture collaborated with Chainlink and RWA.xyz to examine the state of distributed ledger adoption in financial services and provide a perspective on the value of cross-chain capabilities to maximize capital formation, expand distribution channels, promote financing opportunities, and simplify the user experience. This collaboration found that financial services entities are using at least **72** distributed ledgers, with many more expected by 2030.

While this report does not contend that every distributed ledger must interoperate, this research lends credence to the thesis that the number of distributed ledgers in the global financial system will not converge to one ledger to rule them all. **Financial services entities issuing onchain products and services must prioritize cross-chain capabilities to gain a competitive advantage in this evolution in financial markets.**

A Proliferation of Digital Liquidity Islands

The proliferation of digital liquidity islands is increasingly evident and mirrors the Internet's early days when multiple decentralized protocols operated in isolation—until TCP/IP emerged as a universal standard for data transmission. Similarly, distributed ledgers today remain fragmented by technical limitations and the specialized needs of their unique use cases—each requiring distinct levels of security, scalability, privacy, and regulatory compliance.

In this environment, adopting a single distributed ledger remains remote because of the complexities associated with aligning on a single set of standards, balancing incentives, and dismantling competitive barriers. The result is the emergence of so-called Digital Liquidity Islands—with their own distinct assets, applications, and features—that could stall the broader promise of interoperability. Despite these digital liquidity islands benefiting from having access to conventional payment systems for liquidity, this report argues that this source of liquidity is not sufficient and the development of cross-chain interoperability will be paramount to realizing the value of new functionality brought about by tokenization.

[1] For this report, "distributed ledger" refers to the range of public, public-permissioned, and private distributed ledger technologies (DLTs), blockchains, and other smart contract-enabled programmable ledgers.

[2] Financial institutions or financial technology companies, including banks, financial market infrastructures, fintech firms, and payment service providers, with emphasis on those adhering to regulatory frameworks, holding licenses, or being registered with financial supervisory authorities.

[3] Classified as distributed ledgers with their own validators and execution layers and are responsible for storing or making available products and services that have financial value.

[4] Private chains limit participation for confidentiality and compliance, public-permissioned chains allow open auditing while restricting transaction initiation to authorized participants, and public chains enable anyone to participate openly.

In practice, interoperability is like a universal language translator for diverse blockchain networks, enabling them to understand each other and seamlessly exchange value and information. It is how we break down digital barriers, allowing distinct blockchains to collaborate and share identity, money, and objects[5], regardless of their different protocols and rules.

Accenture, Chainlink, and RWA.xyz collaborated to catalog the distributed ledgers used by financial services entities—including financial institutions (“FIs”), financial market infrastructures (“FMIs”), central banks, financial technology companies (“fintechs”), asset and fund managers, payment service providers (“PSPs”), and decentralized finance (“DeFi”) protocols.

> **"Accenture, Chainlink and RWA.xyz Identify at Least 72 Distributed Ledgers Used in Financial Services, with Much More Expected by 2030"**

This analysis found that financial services entities are using at least **72** distributed ledgers based on publicly available information. Of these, 30 are permissionless while the rest are private-permissioned (36), public-permissioned (4), or hybrid (2) implementations. Each distributed ledger uses its own set of validators and/or has a separate execution layer. This list contains distributed ledgers that have executed real-value transactions and are actively or recently used, including limited-phase pilots.

Distributed Ledgers with Financial Services Activity

Distributed Ledger	Type	Codebase	Example Financial Services Entities	Example Use Cases
ADDX	Private	–	ADDX	Tokenized funds
ADB Open Permissioned Blockchain	Public-Permissioned	Cosmos SDK	Asia Digital Bank	Digital assets, DeFi, stablecoins
Algorand	Permissionless	Algorand VM	Bank of Italy, IVASS, Quantoz Payments, National Australia Bank	Digital assets, payments, DeFi, digital guarantees, stablecoins
Aptos	Permissionless	Move VM	Franklin Templeton, Brevan Howard, Hamilton Lane, BlackRock	Tokenized funds
Arbitrum	Permissionless	Ethereum VM	Franklin Templeton, Securitize, Dinari	Tokenized funds, tokenized equities
Avalanche	Permissionless	Ethereum VM	KKR, Citi Group, Franklin Templeton	Tokenized funds
Base	Permissionless	Ethereum VM	Coinbase Asset Management, Dinari, Backed Finance, Franklin Templeton	Tokenized equities
Bitcoin	Permissionless	Bitcoin Core	Ark 21Shares, BlackRock, Bitwise Asset Management, VanEck, WisdomTree, Revolut, etc.	Exchange-traded products
Bitcoin Liquid	Permissionless	Bitcoin Core	STOKR	Promissory notes, carbon credits, security tokens
Blast	Permissionless	Ethereum VM	Dinari	Tokenized equities, digital assets
Canton Network	Private	DAML SDK	Hashnote (Circle), QCP Group, Versana (Bank of America, Barclays, Bloomberg, Citi, Deutsche Bank, JP Morgan, USBancorp, Wells Fargo)	Money market funds, onchain collateral, tokenized credit

[5] According to Accenture, tokenization is impacting a wide range of elements, including digital identity, digital currencies and assets, and digital objects, such as health records and artwork.

Distributed Ledger	Type	Codebase	Example Financial Services Entities	Example Use Cases
Cardano	Permissionless	EUTXO	Franklin Templeton, Sygnum Bank, Acredius	Node operations, staking services
Cashlink	Private	Ethereum VM (Polygon POS)	Kreditanstalt für Wiederaufbau (KfW)	Tokenized bonds
Celo	Permissionless	Ethereum VM	Centrifuge	Tokenized treasuries
Citi Integrated Digital Assets Platform (CIDAP)	Private	Ethereum VM (Besu)	Citi Group	Tokenized deposits, trade finance, FX settlement
CLSNet	Private	Hyperledger Fabric	Goldman Sachs, Morgan Stanley	FX settlement
Concordium	Permissionless	Wasm	Membrane Finance	Stablecoins, DeFi
D7 Platform	Private	DAML SDK	Clearstream, Deutsche Börse, KfW	Tokenized securities, tokenized bonds
DBS Token Services	Private	Ethereum VM	DBS Bank	Tokenized treasuries
Distributed Ledger Repo (DLR)	Private	DAML + VMWare	Broadridge, UBS, HSBC, Société Générale	Collateral repos
Distributed Ledger for Securities Settlement System (DL3S) – pilot	Private	Hyperledger Fabric	Banque de France, European Investment Bank, Goldman Sachs	Collateral repos,, exploratory central bank cash tokens
Digital-FMI	Private	Corda	Euroclear, Citi Group, Asian Infrastructure Investment Bank, World Bank	Tokenized securities
Ethereum	Permissionless	Ethereum VM	BlackRock, Circle, Societe Generale, PostFinance AG, Revolut, Visa	Tokenized funds, tokenized bonds, stablecoins, staking
Finteum	Private	Corda	UBS, Canadian Imperial Bank of Commerce	FX settlement
Fnality Sterling Payments	Private	Ethereum VM (Besu)	Lloyds Banking Group, Banco Santander, UBS	Institutional payments
FundsDLT	Private	Quorum	Clearstream, Deutsche Börse Group	Fund distribution
FX Settlement Solution	Private	Baton Systems CORE Ledger	HSBC, Wells Fargo	FX settlement
Gnosis	Permissionless	Ethereum VM	Monerium	Payments
GS DAP™	Private	DAML SDK + Corda	Goldman Sachs, European Investment Bank	Tokenized bonds, collateral repos
Hedera	Public-Permissioned	Hedera Hashgraph	Archax	Money market funds
HQLAˣ Collateral	Private	Corda	BNY, Goldman Sachs, HSBC	Collateral repos
HSBC Orion	Private	DAML SDK	HSBC, BNP Paribas, Royal Bank of Canada	Tokenized bonds, Tokenized commodities (gold)
iBet	Private	Ethereum VM (Quorum)	Hitachi	Tokenized bonds
iCapital	Private	DAML SDK	UBS	Tokenized funds
Injective	Permissionless	Cosmos SDK	Ondo Finance	Tokenized securities
Ink	Permissionless	Ethereum VM	Apollo Asset Management	Tokenized funds
IOTA	Permissionless	UTXO	Realize	Tokenized securities
IZNES	Private	Hyperledger Fabric	Euroclear	Fund distribution

Distributed Ledger	Type	Codebase	Example Financial Services Entities	Example Use Cases
Kava	Permissionless	Cosmos SDK + Ethereum VM	Tether	Payments
Klaytn	Hybrid	Ethereum VM	Bank of Korea	Central bank digital currencies
Komgo	Private	Ethereum VM (Quorum)	BBVA	Trade finance
LINE	Permissionless	LINE Blockchain	SoftBank	Central bank digital currencies
Mantle	Permissionless	Ethereum VM	Ondo Finance	Real-world assets
mBridge Ledger	Private	Ethereum VM (mBridge Ledger)	Hong Kong Monetary Authority, Bank of Thailand, Central Bank of the United Arab Emirates, People's Bank of China, and the BIS Innovation Hub Hong Kong Centre.	Central bank digital currencies
NEAR	Permissionless	Near VM	Hamilton Lane, Brevan Howard	Tokenized funds
Neutral Trading	Private	Ethereum VM	Neutral and DLT Finance	Carbon credits
Noble	Permissionless	Cosmos SDK	Circle	Real-world assets
Northern Trust Matrix Zenith	Private	Ethereum VM (Besu)	Northern Trust	Digital assets, carbon credits
Kinexys (fka Onyx)	Private	Ethereum VM (Quorum)	JP Morgan, Mastercard, Santander	Tokenized deposits, repurchase agreements
Ondo Chain (testnet)	Permissionless	Ethereum VM	JP Morgan	Real-world assets, tokenized treasuries
Optimism	Permissionless	Ethereum VM	BlackRock	Real-world assets
Partior	Private	Ethereum VM (Quorum)	JP Morgan, Deutsche Bank, Nium, DBS, Temasek	Payments
Polkadot	Permissionless	Polkadot Network	Zodia Custody	Custody
Polygon	Permissionless	Ethereum VM	Hamilton Lane, KfW, Obligate, Apollo Asset Management, AirCarbon Exchange	Tokenized funds, tokenized bonds, on-chain corporate finance, carbon credits
Polymesh	Private	Parity Technologies Substrate	AlphaPoint, DigiClear CSD	Tokenized equities, tokenized funds
Progmat	Private	Corda	Bank of Tokyo-Mitsubishi	Payments
Project mBridge	Private	Ethereum VM	Multiple central banks	Payments
Prometheum ATS	Private	--	Prometheum Capital	Digital asset trading, settlement, custody
Provenance	Permissionless	Cosmos SDK	Apollo Global Management, Hamilton Lane	Tokenized funds
Regulated Liability Network	Private	Corda	Barclays, Citi, HSBC, Lloyds, Mastercard, NatWest, Nationwide, Santander, Standard Chartered, Visa	Payments
Sber Blockchain	Private	Hyperledger Fabric	Sberbank	Tokenized commodities
Six Digital Exchange (SDX)	Private	Corda	Six Group, Swiss National Bank	Tokenized bonds
Solana	Permissionless	Solana VM	PayPal, Nomura, Securitize, Visa	Payments, tokenized funds

Distributed Ledger	Type	Codebase	Example Financial Services Entities	Example Use Cases
Spruce (Avalanche)	Public-Permissioned	Ethereum VM	T. Rowe Price, WisdomTree, Wellington Management, Cumberland	On-chain trading
Stellar	Public-Permissioned	Stellar VM	MoneyGram, DBS Lightcast, SCB	Cross-border payments
Sui	Permissionless	Move VM	Circle, Ondo Finance	Real-world assets
SWIAT	Private	Ethereum VM	Siemens, BayernLB, DekaBank, DZ BANK, Helaba, LBBW	Tokenized bonds
TassatPay	Private	Ethereum VM	Cogent Bank, Customers Bank, Western Alliance Bank	Payments
Tezos	Permissionless	Michelson Liquid	Xalts	Tokenization
USDF Consortium	Private	Cosmos SDK	Various U.S. regional banks (NY Community Bank, NBH Bank, FirstBank)	Payments
XDC Network	Hybrid	Ethereum VM (XinFin)	Neutral and DLT Finance	Tokenized treasuries
zkSync Era	Permissionless	zkVM	Circle	Real-world assets

> *Note: This table provides a snapshot of the distributed ledger landscape for research purposes and is not exhaustive. Example use cases and financial services entities are illustrative and are not intended to be comprehensive.*

Additional Distributed Ledgers on the Horizon

Beyond the 72 distributed ledgers in use today with real-value transactions or limited-phase pilots, there are others that are planned or currently being tested. The following are examples of such:

- The CME Group is testing the Google Cloud Universal Ledger for seamless and secure wholesale payments and tokenization of assets.
- Deutsche Bank announced plans to develop an Ethereum layer-2 distributed ledger using ZKSync technology to adhere to various regulatory compliance measures.
- Ethena and Converge announced plans to launch Converge, an EVM-focused blockchain that will support and advance DeFi and tokenized assets for institutional investors.
- Backed, Sonic and Chainlink announced that they are partnering with Fortlake Asset Management to tokenize their Sigma Opportunities Fund on the Sonic EVM layer-1 blockchain.

While this report sought to capture a comprehensive catalog of the total distributed ledgers in use or planned, some may be excluded.

Expected Continued Diversification Through 2030

This report contends that the financial services industry will continue growing the number of distributed ledgers, driven by a number of market forces occurring across three modalities.

Market Forces Driving Diversification

This research found **ten market forces** that have underpinned the proliferation of digital liquidity islands:

Market Force[6]	Description
Bespoke Standards	Organizations develop unique technical protocols to meet specific requirements, such as privacy, security, or compliance elements, which can hinder cross-chain connectivity.
Competitive Differentiation	Institutions may establish a distributed ledger to gain a first-mover advantage or to capture a specific market, such as a market structure positioning itself as a leader within a specific region or jurisdiction.
Customer Data Protection & Privacy	Requirements to safeguard customer data from bad actors acting on open networks have, at times, driven the design of less interoperable systems to preserve customer safety and privacy.
Economic Feasibility	The cost of deploying distributed ledgers will continue to lower as network and infrastructure designs are optimized and agreeable frameworks are operationalized.
Industry-led Ownership	Increasing demand for industry-owned or -shared distributed ledgers will catalyze the development of shared systems that promote inclusive coordination.
Industry Vertical Focus	Narrowly targeted projects seeking to activate a specific industry vertical, such as collateral markets, may not inherently prioritize broad-based interoperability.
Institutional Risk Tolerance	Driven by mitigating regulatory and operational risk, institutions have historically prioritized permissioned blockchains, ensuring transactions occur with known counterparties.
Regulatory Perimeters	Jurisdiction-specific regulations, such as data localization requirements, often confine distributed ledgers to certain geographical or legal domains.
Settlement Asset Preference	Divergent choices in settlement assets, such as public or private money[7], drive fundamental design choices that could ultimately lead to isolated walled gardens.
Targeted Distribution	Certain institutions may elect to deploy a distributed ledger targeted toward discrete distribution channels, such as specific customer bases.

Modalities for Growth

While independently deployed models will persist, distributed ledgers are primarily expected to grow across three dimensions in financial services.

Vertical ecosystem expansion has been popularized in the Ethereum ecosystem, where layer-2 (L2) and layer-3 (L3) distributed ledgers extend the transaction processing capabilities of the base layer-1 (L1) network. L1s are foundational networks that provide protocols and secure infrastructure and handle core functions like consensus, data availability, and settlement. L2s are distributed ledgers built on L1s that improve scalability by processing transactions offchain before publishing compressed batches of transactions onto the L1 network so the L2 ledger can be independently recreated and verified. The two primary L2 “rollup” models are achieved via optimistic and zero-knowledge rollups, each offering varying benefits and trade-offs.[8] L3s are even more specialized distributed ledgers built on L2s. Optimism's Superchain model, for example, aims to support L3 deployments.[9]

Horizontal ecosystem expansion has been advanced by ecosystems like the Canton Network[10], Avalanche, OP Stack, Cosmos, and Polkadot, where multiple distributed ledgers can be deployed, with each retaining relative sovereignty.

Consortia-led distributed ledgers are shared platforms governed by private sector financial institutions or, in certain cases, central banks or other relevant authorities. Project mBridge, Global Layer 1, and the Regulated Liability Network are examples of such initiatives. In some cases, consortia-led or shared distributed ledgers may catalyze participating institutions or corporations to develop their intra-distributed ledger to manage permissions and liquidity across multiple ecosystems.

[6] Market forces are listed in alphabetical order.

[7] Settlement assets, in this context, describe an onchain asset used to settle a transaction to discharge counterparty obligations. Often, this includes onchain cash, such as deposit tokens or stablecoins, acting as the ‘P’ in a DvP arrangement, for example.

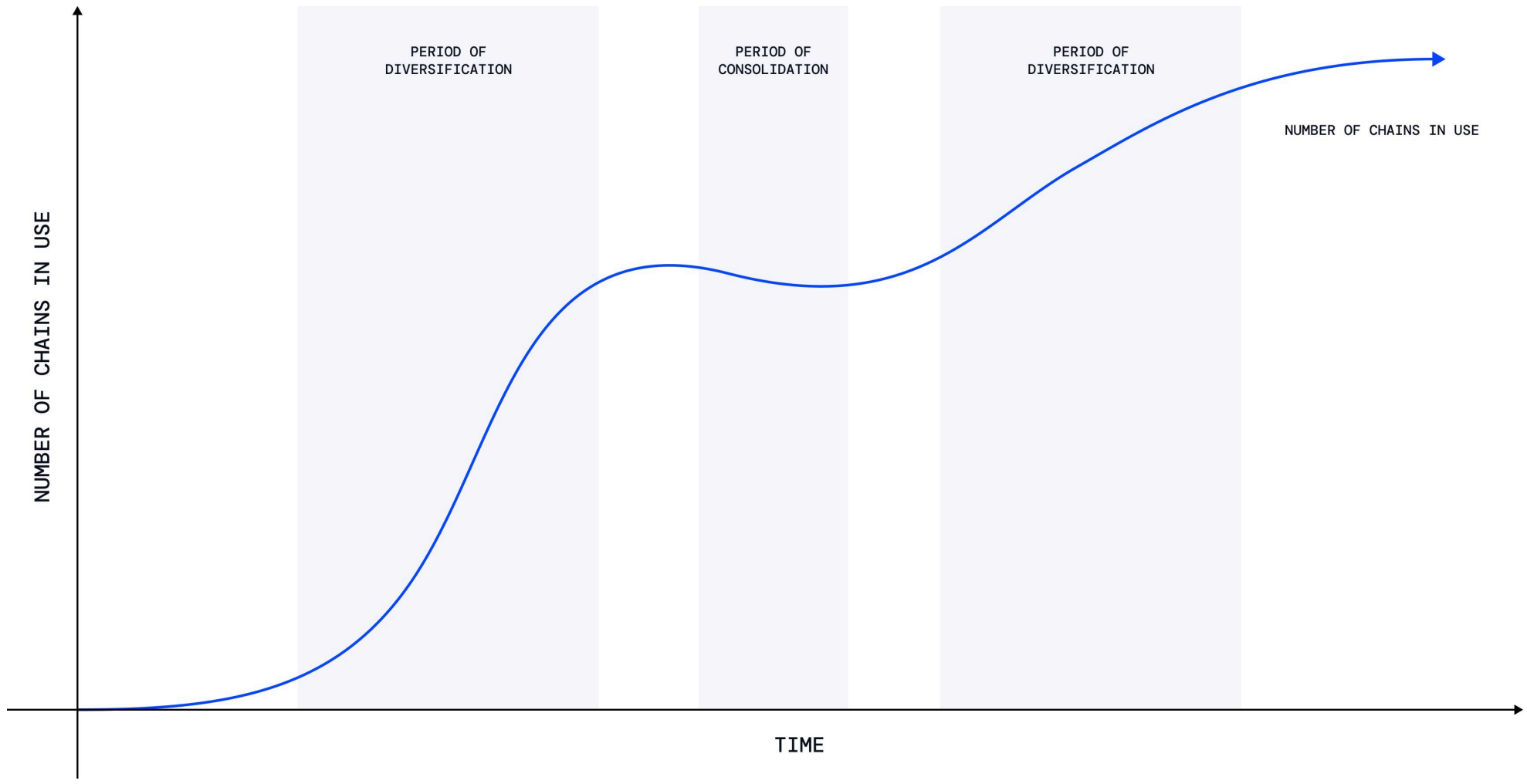
[8] *VanEck. (2024). Ethereum Layer-2s Valuation Prediction by 2030.*

[9] *Crypto Briefing (2024). Optimism will roll out new features to support layer 3 on Superchain.*

[10] *Canton Network. (2024). Insights from the Canton Network Pilot.*

Periods of Diversification and Consolidation

IDC Research predicts that by 2029, 80% of industry ecosystems will leverage blockchain-driven distributed ledgers for multiparty capital workflows, enhancing interoperability, transparency, and cost efficiency.[11] In accordance, also, the number of distributed ledgers used by financial services entities is expected to grow through 2030. However, this growth will experience periods of diversification and consolidation. During these periods, the market role of interoperability service providers will evolve as market demands change.



Illustrative: Expected periods of diversification and consolidation of distributed ledgers in financial services

During periods of **diversification**—or growth in distributed ledgers—financial services entities will add to the total value and information available onchain, increasing the risk of new distributed ledgers becoming digital liquidity islands. Firms seeking to ensure seamless communication and liquidity flows across other chains will preempt and mitigate this risk and build using industry standards for interoperability. In these periods of diversity, interoperability service providers will act as the connective tissue, offering "interoperability as a service," acting much like a financial market utility[12].

Periods of **consolidation**—or a decrease in distributed ledgers—will be driven by structural changes, such as technology innovations, competitive pressures, and regulatory changes. These cycles could lead to inactive distributed ledgers across public and private deployments, which could drive interoperability service providers to migrate information and value from one distributed network to another.

The Value of Interoperability

Current state interoperability in financial markets relies on commonly accepted technology standards and market governance or practices and can be achieved in many ways. For example, Swift, a global member-owned cooperative and the world's leading provider of secure financial messaging services has developed standards for international bank transfers and communication between financial services entities and has evolved them to support models, patterns, and messages to support the community's real-time demands more effectively. Another example is ISO 20022, the global standard for sending payment instructions between local, regional, and international financial services entities; it defines building blocks and design patterns for the development of payment messages through a common platform methodology, process, and repository.

[11] DC FutureScape: Worldwide Future of Industry Ecosystems 2025 Predictions, October 28, 2024.

[12] In this context, an interoperability service provider or solution could act as a financial market utility that facilitates the secure and efficient transfer, clearing, or settlement of onchain assets across distributed ledgers to ensure market connectivity and liquidity.

Conversely, programmable distributed ledgers are smart contract platforms that can execute business logic and deliver value in multi-party constructs governed by a framework unique to the use case, business arrangements, and counterparties. Interoperability with external distributed ledgers or ecosystems is not always a natively available feature for public and private deployments. In most cases, efforts must be made to transfer value and information across chains.

Interoperability's objective is to support the trading and transferring of digital assets (or tokens) from one blockchain to another without compromising the security of the source or destination chain.

This research found that effective and scaled cross-chain interoperability can drive the following benefits:

- **Boost Market Liquidity**: Connecting fragmented ecosystems unlocks larger addressable markets and greater capital for onchain financial products.
- **Eliminate Data and Value Silos**: Interoperable blockchains break down institutional barriers, enabling frictionless data exchange and value transfer.
- **Activate Network Effects**: Interoperable platforms increase visibility and adoption, as customers across institutions can easily access financial products.
- **Reduce Costs via Orchestration**: Automated, highly programmable cross-chain workflows replace manual, siloed processes, reducing operational expenses and unlocking new financial services.
- **Simplify the User Experience**: Seamless interoperability encourages wider adoption by streamlining the user journey for tokenized financial services.

Chainlink CCIP: The Standard for Cross-Chain Interoperability

The Chainlink Cross-Chain Interoperability Protocol (CCIP) addresses the emergence of digital liquidity islands by providing seamless cross-chain communication, value transfer, and real-time data synchronization between blockchains and with offchain systems. CCIP enables financial services entities to integrate across independent distributed ledgers and with conventional networks while aiding security, transparency, and regulatory compliance.

CCIP offers multiple modalities for validating and executing cross-chain token transfers: Burn & Mint, Burn & Unlock, and Lock & Mint. For more information on CCIP's various interoperability modalities, refer to Understanding Cross-Chain Token Transfers.

Chainlink's modular architecture allows for tailored interoperability solutions based on specific business needs. Chainlink Labs works with institutions to develop bespoke interoperability solutions that support compliance with regional regulations, privacy requirements, and industry standards. Chainlink CCIP is uniquely suited for connecting both distributed ledgers and existing financial systems to distributed ledgers given its security-first approach through the use of decentralized oracle networks (DONs) to validate each cross-chain transaction, the independent Risk Management Network for secondary validation, and blockchain-agnostic architecture.

For example, CCIP enables seamless USDC transfers between up to 14 distributed ledgers by burning tokens on the source chain and minting them on the destination chain, enhancing cross-chain interoperability without the need for wrapped assets.

Composable Interoperability with the Chainlink Runtime Environment

As the complexity of financial systems and blockchain networks grows, institutions require infrastructure that not only connects systems, but also enables flexible and secure workflow composition that can coordinate activity across blockchains. The Chainlink Runtime Environment (CRE) is a new execution layer of the Chainlink Platform that allows developers to build, test, and deploy customized cross-chain workflows that integrate with multiple blockchains and Chainlink services, including CCIP, Data Feeds, Proof of Reserve, and more.

With CRE, institutions can configure secure, repeatable flows that move data and value across distributed ledgers, while automating decisions based on real-time external inputs and risk signals. CRE enables developers and architects to:

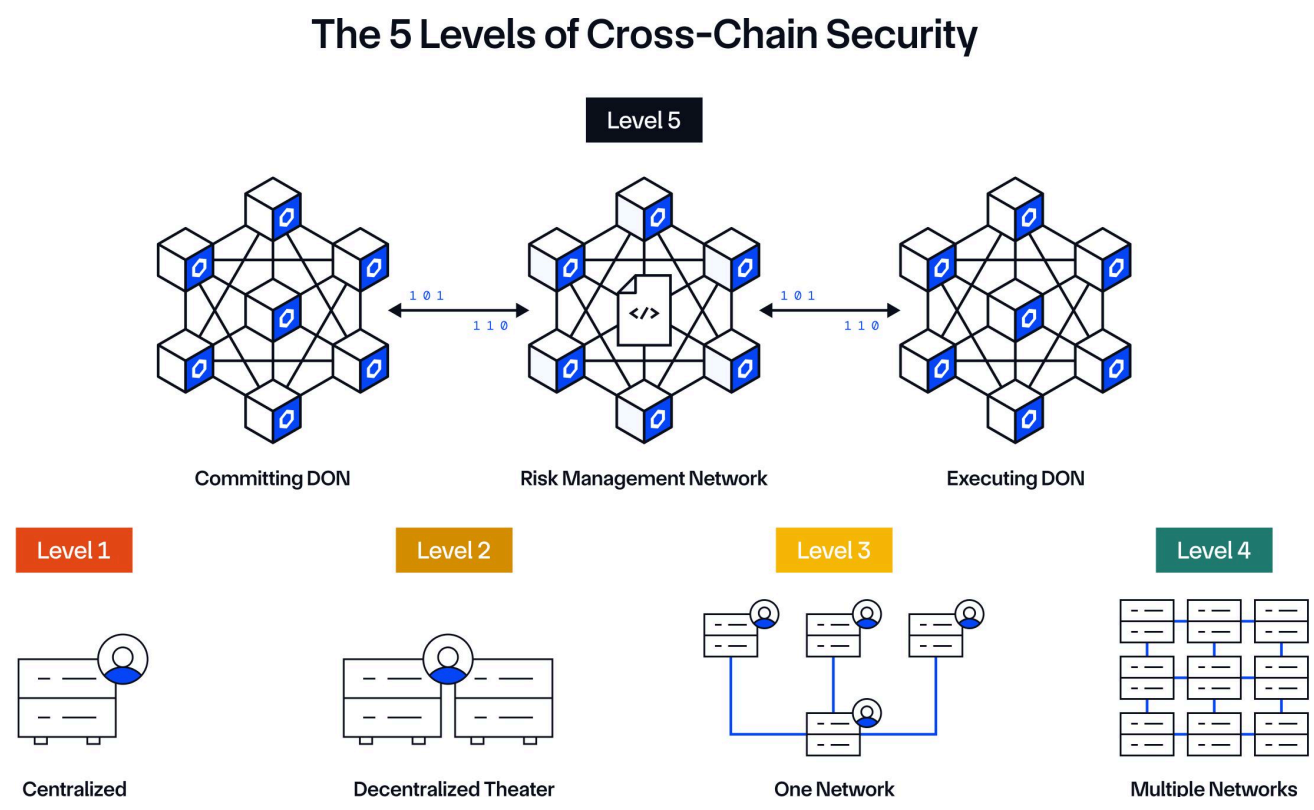
- Compose multi-service workflows using modular, blockchain-agnostic building blocks.
- Simulate and validate cross-chain interactions in a controlled environment.
- Deploy and scale production-grade interoperability solutions with security and compliance built-in.

By abstracting away the complexities of managing different blockchains, message formats, and execution environments, CRE supports the rapid development of interoperable applications that align with enterprise governance, privacy, and regulatory requirements. CRE serves as the foundation for financial institutions to operationalize the benefits of interoperability at scale—delivering seamless asset movement, data synchronization, and smart contract orchestration across public and private networks—with these workflows being able to easily integrate with existing legacy systems.

Blockchain-to-Blockchain Connectivity

Chainlink CCIP enables arbitrary messaging between disparate blockchains, allowing smart contracts to send data and commands between chains to enable cross-chain applications. CCIP also supports secure token transfers between blockchain networks through the Cross-Chain Token (CCT) standard, where any token issuer can integrate cross-chain capabilities into their token in a completely self-serve manner. The CCT standard does not impose vendor lock-in on token issuers and was built to support established token standards like ERC20, but is also flexible enough to support customized token deployments. CCIP also supports programmable token transfers, enabling the transfer of both value and data cross-chain, where the message informs smart contracts on what to do with the tokens once they arrive on the destination chain (e.g., swap the token for another and stake it).

Chainlink's CCIP implements Level-5 cross-chain security through multiple decentralized networks that collectively secure individual cross-chain transactions. The system employs three distinct decentralized networks: a Committing DON, an Execution DON, and a Risk Management Network, each operated by independent node operators with separate key holders and responsibilities. The protocol uses two separate codebases written in different programming languages, providing client diversity and decentralization in its cross-chain infrastructure.



The Risk Management Network operates independently from the transactional Decentralized Oracle Networks (DONs) and provides active monitoring and risk mitigation capabilities by providing a secondary, independent validation of cross-chain transactions. The combination of multiple independent verification layers, separated responsibilities among node operators, and a defense-in-depth approach to risk management enables CCIP to achieve Level-5 security in cross-chain interoperability for token transfers and messaging across blockchain networks.

Conventional System Connectivity and Private Cross-Chain Transactions

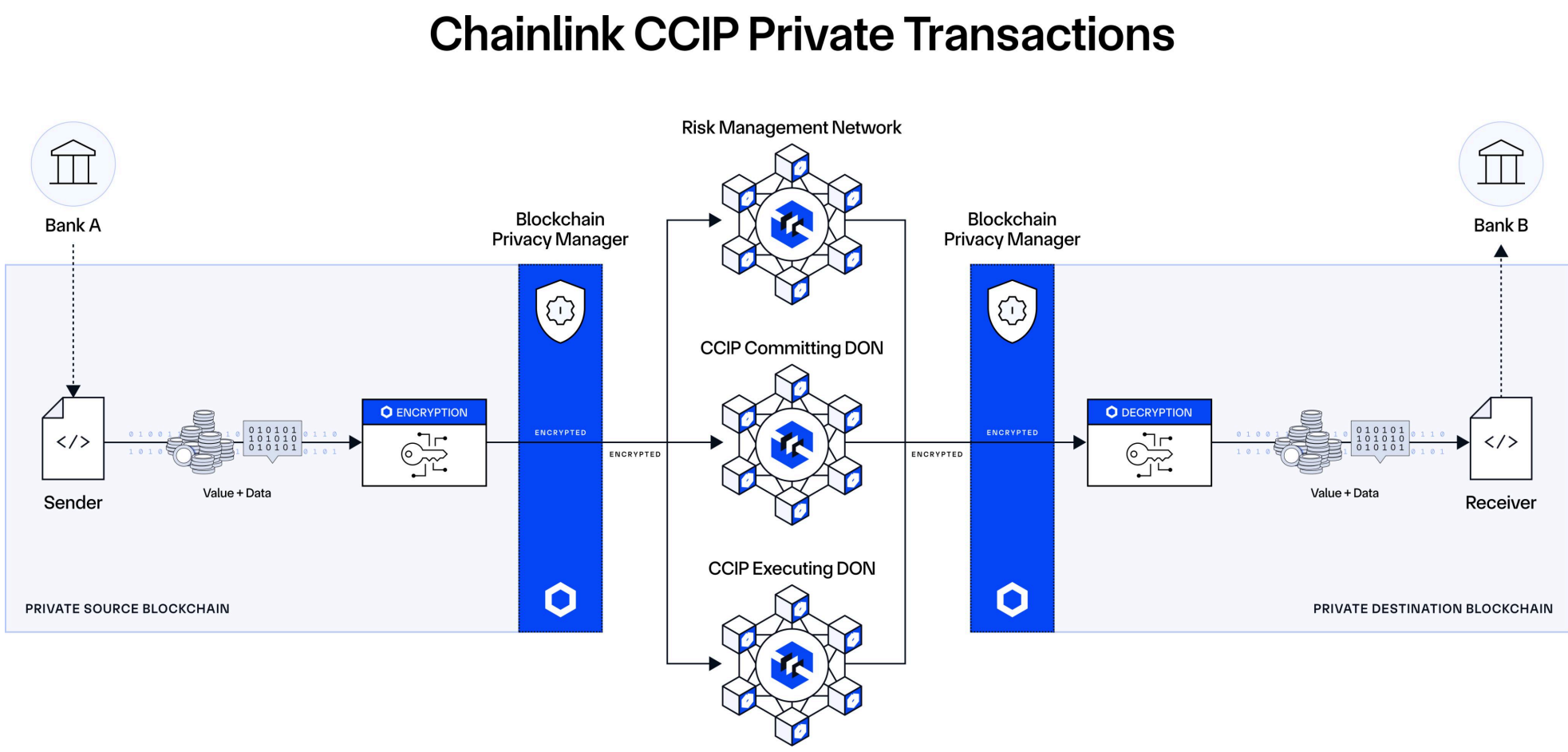
The Chainlink platform facilitates connections between traditional financial systems and blockchain networks through services such as the Blockchain Privacy Manager, which enables institutions to integrate private blockchain networks with existing enterprise systems while maintaining confidentiality of private chain data. This infrastructure allows FIs to control and limit data exposure, protecting sensitive information while enabling necessary cross-system communication.

Key financial market infrastructures and institutions such as Swift, Fidelity International, and ANZ Bank are using Chainlink CCIP as well as top DeFi protocols including Aave and Lido.

Case Study: Private Cross-Chain Token Transfers with ANZ Bank

Built upon the Blockchain Privacy Manager, Chainlink's CCIP Private Transactions addresses a crucial privacy challenge in private blockchain interoperability, and is being used by ANZ Bank under MAS Project Guardian. The solution enables banks to conduct confidential cross-chain transactions for tokenized real-world assets on private chains while supporting regulatory compliance with GDPR and MiFID II. By facilitating secure interactions between private institutional chains, this innovation can accelerate institutional blockchain adoption.

Built upon the Blockchain Privacy Manager, CCIP Private Transactions employs encryption for both asset data and value, supporting privacy at the network level and during transit. Allowing banks to maintain full data confidentiality while transacting between private blockchain networks enables them to meet the strict confidentiality requirements of FIs. Furthermore, the Blockchain Privacy Manager enables institutions to connect private chains to public blockchain networks, while maintaining privacy over private chain data by defining the exact scope of information that is necessary to reveal to enable cross-chain transaction processing.



Building Cross-Chain Capabilities

Cross-chain interoperability at scale is more than a technology solution—it requires strategic visioning to bolster the product roadmap, careful smart contract engineering, treasury and liquidity management capabilities, and a robust governance and operating model to oversee activities.

Business Drivers

Leaders of financial services entities with onchain financial products and services should consider the following drivers for evaluating their cross-chain strategies:

1. **Accessing Capital and Liquidity**: How might we incentivize the injection of investor capital to drive customer demand, ensure liquidity depth, and enhance price discovery for our onchain financial products?
2. **Expanding Distribution**: How might we activate and engage a broader cross section of investors/customers to enhance the reach of our onchain financial products?
3. **Increasing Financing Opportunities**: How might we empower our investors/customers to collateralize assets across chains and securely realize the power of leverage?
4. **Optimizing the User Experience**: How might we ensure our customers experience smoother transactions across distributed ledgers without complex bridging requirements?
5. **Complying with Reporting Requirements**: How might we ensure we transmit information across distributed ledgers, such as trading activity, to meet various reporting requirements and compliance measures?

Addressing these areas—from capital and distribution channels to financing and product optimization—will lead firms to consider cross-chain capabilities to drive customer engagement. This report contends that a financial institution will undergo four stages to realize cross-chain capabilities.

Approach to Becoming a Cross-Chain Financial Institution

	Key Activities
Business Case & Cross Chain Architecture Blueprint	• Evaluate organizational readiness, ensuring leadership alignment on interoperability goals and clarifying the near and long term business case. • Considering how cross chain capabilities in new and existing products will enhance value proposition for customers by drafting and revising business case for new and existing products. • Design a feature ready cross-chain architecture, aligning technology choices (e.g., interoperability protocols, network selections) with business goals. • Incorporate platform neutrality principles, enabling collaboration across a diversity of chains to enable extensibility and mitigate technical debt.
Smart Contract Engineering	• Embeded specialized engineering support across various smart contract platforms (e.g., EVM, SVM), ensuring seamless integration with your existing systems. • Build compliance features (e.g., freezing funds, allow/deny lists) and advanced testing procedures to mitigate risk, depending on the use case and risk profile. • Coordinate periodic external audits and bug bounty programs to confirm contract integrity, reduce attack vectors, and ensure adherence to privacy requirements.
Treasury & Liquidity Management	• Deploy treasury management solutions that handle real time balance monitoring and settlement across diverse blockchains. • Enable stakeholders to evaluate and route transactions to the most efficient or compliant network, reducing operational friction and liquidity risks. • Integrate conventional and legacy systems with tokenized systems to mitigate the occurrence of multiple liquidity pools unnecessarily (intra-enterprise fragmentation).
Governance & Operating Model	• Develop robust enterprise policies and protocols for managing access controls, transaction limits, and conflict resolution across multiple chains. • Insitute key management practices within the enterprise, including embedding collaborative and managed custody practices as needed. • Implement performance monitoring and reporting to track value flows across networks, and create contingencies for incidents, such as customer support functions.

Business Case and Cross-Chain Architecture Blueprint

A robust cross-chain vision begins by building a business case and assessing how blockchain interoperability benefits the existing product roadmap. By articulating the value interoperability can bring to you and your customers, you can begin to align on an approach to integrating this new infrastructure into your business. Institutions can use platforms such as Chainlink, which offers modular, interoperable infrastructure capable of supporting compliance-focused, multi-network workflows and aligning with long-term strategic goals. Bringing diverse stakeholders from product, technology, and compliance is critical for defining clear objectives, KPIs, and design principles linked to a business case. Measuring the volume and performance of cross-chain adoption can drive real-time insights into how onchain assets enable product optimization.[13]

Platform neutrality[14] is emerging as a key priority, allowing institutions to integrate preferred blockchain networks while preserving their sovereignty and flexibility for future innovations. A compliance-focused approach—covering KYC/AML, data privacy, and other regulations—should be woven into every stage of development. Organizational change impact assessments prepare teams for the demands of multi-chain environments, ensuring operational readiness for new capabilities and processes.

With a carefully crafted blueprint, institutions gain a clear roadmap for leveraging cross-chain interoperability to boost efficiency, elevate customer experiences, and secure a leading market position.

Smart Contract Engineering

Smart contracts are the driving force behind the automation, security, and trust enabled by modern blockchain solutions. Engineering efforts begin by selecting the appropriate virtual machine—often the Ethereum Virtual Machine (EVM) or Solana Virtual Machine (SVM)—and employing languages like Solidity or Rust.

To streamline development and reduce complexity, the Chainlink platform offers a suite of capabilities, decentralized services—including CCIP—and supporting development tools. The Chainlink Runtime Environment serves as the execution engine that enables developers to compose, simulate, and deploy custom workflows by orchestrating modular capabilities in a decentralized manner.

Engineering and product teams must then work closely with the business to translate in-scope business processes and product features into purpose-built smart contracts. Compliance features should be explored, including fund-freezing and transfer-blocking mechanisms to maintain sanctions compliance. Clawbacks, privacy controls, and permissioned token standards can all be leveraged as tools to tailor smart contracts to meet business and compliance requirements.

Rigorous testing, augmented by third-party audits and bug bounty programs, helps detect and mitigate vulnerabilities. Combining static and dynamic analyses (e.g., automated code scans, unit testing, and scenario planning) ensures comprehensive coverage of potential risks. Both static and dynamic analyses should be incorporated to capture the gamut of variabilities that could be encountered, including automated code scanning, unit testing, and scenario planning. Handling sensitive data often requires offchain storage or advanced cryptographic solutions to align with privacy regulations. Coordinating contract logic with enterprise systems streamlines reconciliation, asset transfers, and settlements more efficiently than traditional approaches.

By utilizing the Chainlink platform, engineering teams can enhance efficiency, ensure interoperability, and develop robust smart contract architectures that seamlessly integrate with both distributed ledger networks and traditional financial systems.

[13] The growth and volume of interoperability can be measured through (1) the total number of messages and (2) the total value of assets transferred between distributed ledgers.

[14] Platform neutrality ensures that systems operate with credible neutrality—transparent, unbiased, and free from favoritism—fostering broader participation, like how the universally accessible and impartial email protocol enables innovation and collaboration across institutions.

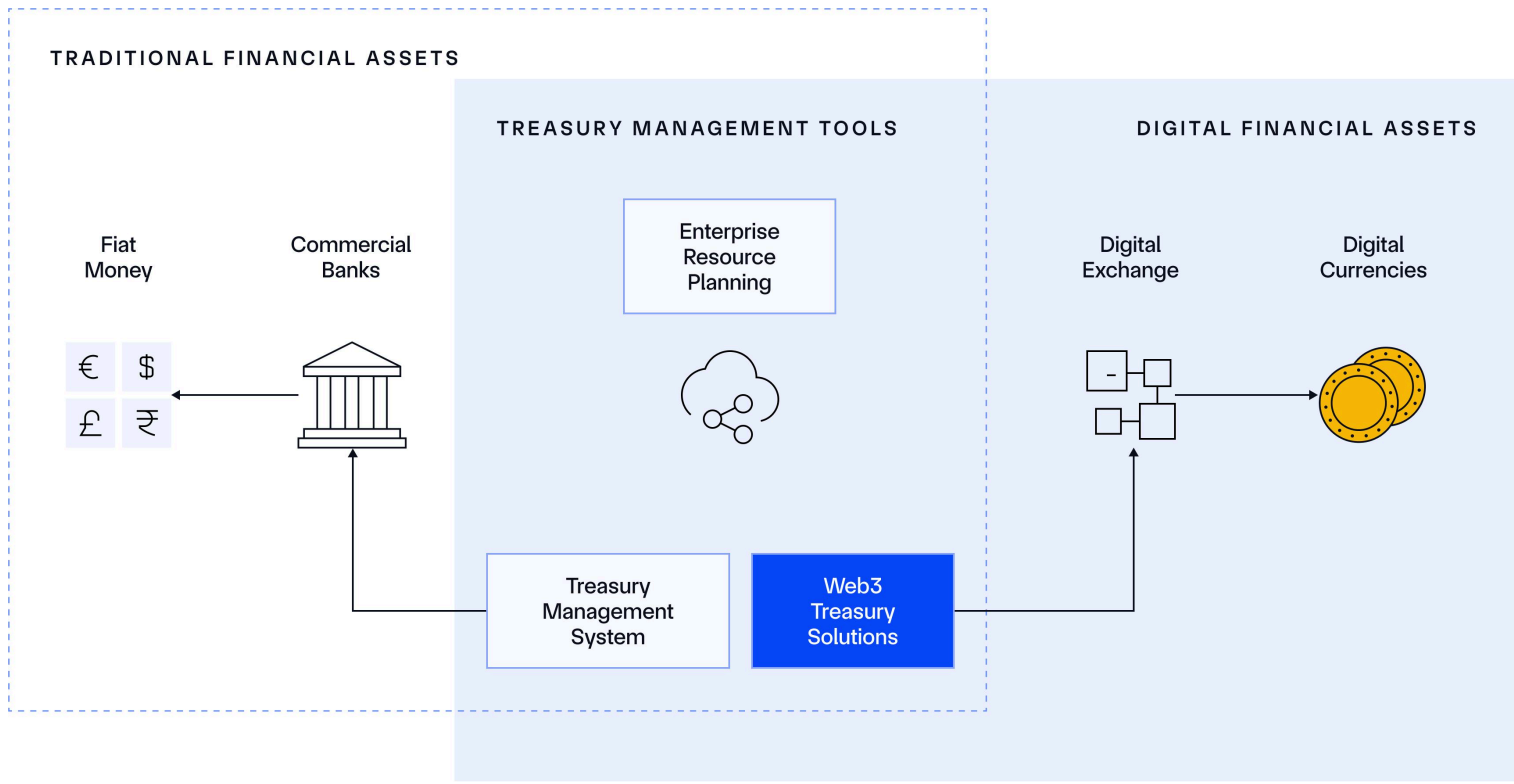
Treasury & Liquidity Management

Modern treasury operations increasingly span traditional banking channels and emerging blockchain networks. A comprehensive strategy employs a Treasury Management System (“TMS”), Enterprise Resource Planning (“ERP”) platform, and a dedicated Web3 treasury solution to offer real-time visibility of both fiat and tokenized assets. This integrated viewpoint provides treasurers the sight lines to choose the most cost-effective and compliant payment rail for each transaction.

Aggregator layers can be introduced to consolidate positions across multiple chains, simplifying monitoring and decision-making. Embedding Know Your Transaction (KYT), and identity verification mechanisms maintain regulatory compliance while minimizing disruption to operations. Gas-fee abstraction models allow fees to be paid in various tokens or sponsored by the institution, fostering a better user experience.

From large-scale corporate payments to cross-border settlements, a unified treasury approach reduces overhead and provides strategic agility—institutions can swiftly reallocate liquidity and respond to evolving financial possibilities.

Cross-Chain Treasury Management



Governance & Operating Model

Successful cross-chain initiatives demand a governance structure and operating model capable of managing intricate risks and technological challenges. Well-defined governance policies regulate user access, validate transactions, and track consensus across multiple distributed ledgers. These policies should also anticipate threats such as 51% attacks[15] to ensure the security of assets across chains.

Tiered monitoring, escalation, and incident-handling frameworks enhance operational efficiency, from routine performance checks to rapid interventions for critical issues. Gas-fee abstraction[16] at this governance layer further promotes user adoption by allowing transaction fees to be paid in diverse tokens or absorbed by the institution, all while adhering to KYC/AML and data privacy mandates.

Beyond technical oversight, a well-structured operating model clarifies organizational roles, training, and change management to coordinate IT, compliance, finance, and customer support efforts. Integrating contingency planning and performance monitoring builds resilience, helping institutions adapt to shifting regulations while delivering consistent, secure services in a dynamic financial landscape.

[15] A 51% attack occurs when a single entity gains control of more than 50% of a blockchain’s mining or validation power. This allows the entity to manipulate transactions by double-spending or censoring new transactions, undermining the network’s integrity.

[16] Gas fee abstraction enables users to pay transaction fees in different tokens or have them covered on their behalf, simplifying gas management and user experience. Public blockchains typically require gas fees paid in native tokens (e.g., ETH), while private chains have more flexibility in fee structures. This approach could enable financial services entities to navigate compliance risks associated with the custody of native tokens and possible exposure to sanctioned entities.

Getting Started

7 no-regret actions to seize the cross-chain opportunity in 2025:

1. **Craft your onchain product strategy** to drive trust and determine how cross-chain capabilities can enhance the customer experience.

2. **Perform market research and analyze competitive intelligence** to understand evolving customer demands, technology solutions, and competitor strategies.

3. **Engage with key internal and external stakeholders** to gather input, address feasibility concerns, and align on strategic priorities.

4. **Define key cross-chain use cases to address customer demand and pain points** while maximizing competitive differentiation.

5. **Quantify the business case to establish goals and metrics** for monitoring the ROI of cross-chain capabilities, including cost savings and revenue growth.

6. **Develop a proactive risk mitigation plan** to minimize liquidity, compliance, vendor lock-in, and privacy risks associated with cross-chain capabilities.

7. **Ideate a proof-of-concept use case** to drive early lessons learned and enterprise familiarity with onchain products enabled by cross-chain capabilities.

Conclusion

The convergence of traditional and decentralized finance is poised to transform how financial services entities interact with their customers and ecosystems, providing new opportunities for optimizing liquidity, reducing costs, and mitigating risks. However, the continued proliferation of both private and public distributed ledgers can unintentionally create silos of liquidity that could otherwise undermine the potential of such a globally-connected system. While not all distributed ledgers require interoperability, the industry is expecting continued growth and therefore, cross-chain capabilities will become a critical competitive differentiator for financial services entities.

Financial services entities prioritizing secure, flexible cross-chain capabilities early in their tokenization journeys will gain a sustained competitive advantage over those siloed within their walled gardens. By embracing blockchain platform neutrality and interoperability solutions, the debate between public and private distributed ledgers will fade as the focus is rerouted toward enabling the financial sector's open, seamless, and secure unification.

Industry roles will evolve, necessitating new strategies and tools to navigate this complex landscape. Technologies like Chainlink's interoperability standard will be crucial in this transition, providing the necessary infrastructure to support seamless integration and optimized liquidity deployment. As the execution engine of the Chainlink platform, the Chainlink Runtime Environment (CRE) enables institutions to build, test, and operate secure cross-chain financial applications in a programmable and policy-aware environment.

Ultimately, the future of finance will depend on the successful integration of interoperability standards, requiring a concerted effort from technology providers, standards-setting bodies, and the financial sector.

Disclaimer

This report presents an objective analysis of available data, and it is not intended as an endorsement by Accenture of any particular viewpoint or solution.

Examples of financial entities in Table 1 include FIs, FMIs, FMUs, fintechs, payment service providers, investment firms, and other entities engaged in financial services, particularly those adhering to regulatory frameworks and holding licenses or being registered with the relevant financial supervisory authorities or regulators. This encompasses regulated financial institutions, such as commercial banks and investment firms subject to strict oversight, licensed and registered fintech companies providing financial products, services, and platforms operating under the oversight of financial regulators to ensure compliance with relevant legal and regulatory requirements. Some entities may collaborate with regulated actors to offer compliant DeFi products that meet regulatory standards. The regulatory and compliance landscape constantly evolves and varies by region and jurisdiction. This report strives to capture these variations by providing a comprehensive, actionable list of "Financial Services Entities" as a general classification, reflecting the best available understanding of the current frameworks.

Get Started with Chainlink CCIP Today: https://docs.chain.link/ccip

Learn More About Accenture's Blockchain & Web3 Services

accenture

IN COLLABORATION WITH

Chainlink

ACKNOWLEDGMENTS

Accenture

Duane Block
Managing Director
duane.j.block@accenture.com

Cameron Nili
Senior Manager
cameron.nili@accenture.com

Alexei Mojeiko
Senior Consultant
alexei.a.mojeiko@accenture.com

Ashna Shah
Senior Analyst
ashna.shah@accenture.com

Chainlink

Angela Walker
Global Head of Banking & Capital Markets
angie.walker@smartcontract.com

Jimmy Haight
Tokenization Marketing
jimmy.haight@smartcontract.com

Thomas Chanter
Writer & Researcher, Capital Markets
thomas.chanter@smartcontract.com

RWA.xyz

Adam Laurence
Co-founder
adam@rwa.xyz

Bryan Choe
Researcher
bryan@rwa.xyz