Beyond public vs. private chains:

The Prividium breakthrough

Enterprise-grade private, permissioned L2s on Ethereum

Contents

Introduction

Imagine a financial system where cross-border payments settle in seconds, where liquidity moves without friction, and where sensitive data stays private, yet regulators retain the visibility they need. This is no longer theoretical. ZKsync Prividiums make it possible today.

Legacy financial systems immobilize trillions in idle capital and rely on fragmented networks of intermediaries. Public blockchains offer openness and programmability but cannot meet the privacy, compliance, or throughput demands of global financial institutions. Private blockchains provide control but create silos, preventing true interoperability. While each model offers certain capabilities, none provide a fully comprehensive solution.

Prividiums combine the best of all worlds. They are private, permissioned Ethereum-secured Layer 2s, purpose-built for institutions. Powered by ZK proofs, they guarantee confidentiality while ensuring integrity. Transactions execute with atomic finality, eliminating settlement risk. Costs are orders of magnitude lower than legacy rails, and throughput reaches enterprise scale.

Over five workshops, more than 35 leading institutions in the financial industry observed these capabilities in live demonstrations. Two use cases, cross-border payments and intraday repo, proved that Prividiums deliver what no other system can: private, interoperable, near-instant settlement anchored in the security of Ethereum.

Prividiums are not just an incremental improvement. They represent a fundamental redesign of financial infrastructure, one that unlocks liquidity, reduces operational risk, and positions enterprises for the digital economy.

Executive Summary

The financial system is at an inflection point

Cross-border settlement can still take days, immobilizing trillions of dollars in idle accounts. Intraday repo markets are still constrained by cutoff times and manual reconciliation. Even with decades of investment, legacy rails are unable to deliver the privacy, speed, and always-on liquidity that modern institutions require.

Blockchain technology promised to change this, but adoption has been slow and network effects are required. Public blockchains offer openness and programmability, but they cannot satisfy the strict privacy, compliance, and throughput standards of regulated financial institutions. Private ledgers provide control, but at the cost of interoperability, creating silos of liquidity that prevent global scale. Each approach solves part of the problem, but none solves it fully.

Prividiums are different

Prividiums are private, permissioned Ethereum-secured Layer 2s, purpose-built for institutions. Powered by ZK proofs, Prividiums allow confidential transactions to be verified on Ethereum without revealing any sensitive data. Costs are orders of magnitude lower than legacy rails, and throughput reaches enterprise scale, with 10,000+ transactions per second (TPS) at sub-second latency per Prividium. Multiple Prividiums can be seamlessly connected to meet higher scalability requirements. Institutions retain full privacy and control, while still benefiting from Ethereum's global security and auditability.

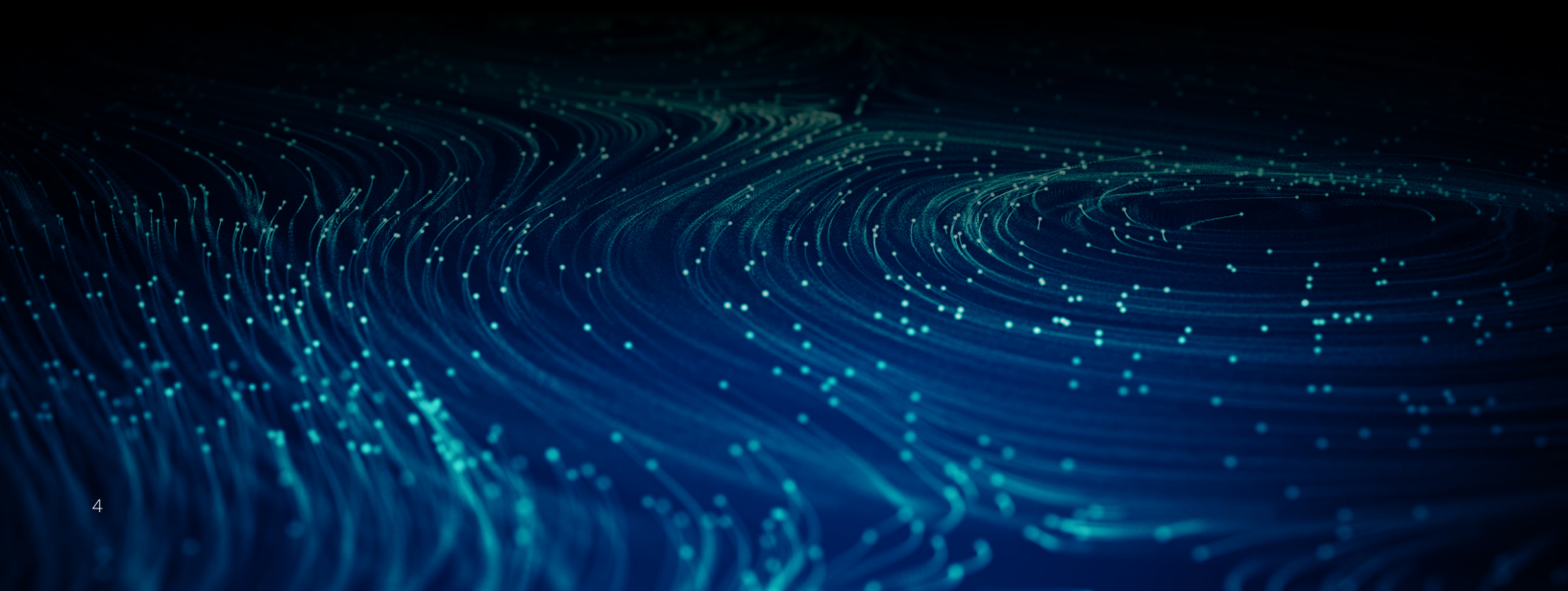
To validate these capabilities, Matter Labs, the core contributors to ZKsync, convened a group of 35+ peer institutions, each representing a diverse set of financial services firms across the globe. In live demonstrations, facilitated by a third-party consultant, participants tested two high-impact use cases:

- **Cross-border payments:** Enabling near-instant, private settlement between enterprise-controlled Prividiums, without reliance on correspondent banking networks.
- **Intraday repo:** Delivering automated, atomic, and private settlement with continuous 24/7 liquidity.

The results: Prividiums reduced reliance on intermediaries, unlocked capital efficiency, and eliminated timing mismatches, while maintaining full privacy, compliance workflows, and regulatory auditability.

How does it work?

By leveraging advanced ZK proof technology, Prividiums enable confidential, trust-minimized, and cost-efficient transactions, ensuring that sensitive data remains protected while maintaining transparency and privacy for regulatory needs. Role-based access controls and built-in compliance workflows support robust anti-money laundering (AML), know-your-customer (KYC), and audit requirements, while the network of interconnected Prividiums enhances connectivity and collaboration across institutions.



At the core of the Prividium design is a middleware layer that aggregates cross-chain messages and ZK proofs, compressing transaction details into a single Ethereum-verifiable proof. This architecture significantly reduces on-chain costs and latency for privacy-preserving Prividiums, while safeguarding sensitive business logic and transaction data. Aggregated proofs are anchored to a shared smart contract on Ethereum, enabling institutions to benefit from the full security and auditability of the public settlement layer without disclosing confidential transaction details. The result is a flexible, scalable, and interoperable platform that bridges the gap between public and private blockchain networks, empowering financial institutions to operate with greater efficiency, privacy, and control.

Demonstrated use cases

The cross-border payments case highlighted the inefficiencies of current correspondent banking models, where multiple intermediaries, pre-funded nostro and vostro accounts, and jurisdictional fragmentation result in slow, costly, and opaque transactions. Prividiums demonstrated the ability to enable near-instant, privacy-preserving settlement across independent, bank-operated chains, consolidating liquidity and reducing the need for prefunded nostro and vostro accounts due to the presence of liquidity pools held at a financial market infrastructure (FMI) chain. By anchoring transaction proofs to Ethereum, Prividiums provide tamper-proof settlement finality while maintaining institutional privacy and regulatory compliance. This approach not only accelerates settlement times and reduces costs, but also enhances transparency and auditability for all parties involved.

The intraday repo use case addressed the operational complexity and risk inherent in today's short-term secured financing markets, particularly in the case of cross-border funding requests. Current workflows rely on a complex web of custodians, correspondent banks, and manual processes, leading to settlement delays, collateral lockup, and increased daylight credit risk. Prividiums enabled automated, atomic settlement of repo transactions via smart contracts, delivering continuous, 24/7 liquidity access and eliminating timing mismatches between cash and collateral legs. This end-to-end automation reduced manual intervention, accelerated settlement, and enhanced capital efficiency, while providing robust audit trails and compliance controls.

Throughout each workshop, participants validated the capabilities of ZKsync Prividiums against each use case, providing feedback on operational, regulatory, and integration considerations. The collaborative approach ensured that the perspectives and requirements of a diverse set of institutions were reflected within the report's findings. Key takeaways from the industry workshops included the importance of establishing robust governance frameworks, the need for streamlined onboarding procedures to ensure AML/KYC capabilities are in place, the integration with legacy systems, and the critical role of regulatory alignment in supporting broader adoption. The group also identified the potential for Prividiums to support additional use cases and may look to engage with additional market participants in a future phase of work.

The future of financial market infrastructure

ZKsync Prividiums represent a significant advancement in the evolution of financial settlement infrastructures. By combining privacy, compliance, scalability, and interoperability within a single, customizable platform, Prividiums address long-standing pain points and unlock new opportunities for efficiency, security, and innovation. The collaborative industry engagement described in this report demonstrates both the technical viability and strategic relevance of Prividiums for modern financial markets. As adoption grows and technology continues to mature, Prividiums are poised to play a central role in shaping the future of financial services, enabling institutions to meet the demands of an increasingly digital and interconnected global economy.

- **Public L1s** = shared state, transparent, bottleneck
- **Private ledgers** = siloed
- **Prividiums** = many private, interoperable chains anchored to Ethereum

Advancing privacy and interoperability in financial services

In today's rapidly evolving financial landscape, the need for secure, scalable, interoperable, and privacy-preserving solutions has never been more pressing. To address these challenges, Matter Labs brought together a variety of financial services organizations across the globe to participate as part of a collaborative industry project. The initiative centered on a series of workshops focused on exploring how privacy and interoperability can coexist on a scalable, Ethereum-secured network, leveraging the latest advancements in ZKsync technology.

Who was involved

The core working group members are comprised of 35+ peer institutions, representing a diverse set of financial services firms across the globe. The goal of this initiative was to create a forum where these participants can observe, engage, and contribute to the development of a next-generation blockchain settlement solution, specifically, Interoperable Prividiums powered by ZKsync. Representatives from global banks, regional banks, asset managers, and crypto-native firms comprised the working group, with workshops facilitated by a third-party consultant and engagement from Matter Labs to provide technical moderation and subject matter expertise throughout the process. Working group participation does not imply any use of the technology presented, now or in the future.

Why we came together

The motivation for convening a large, diverse group of organizations was rooted in a shared recognition of the financial services industry's need to address two critical challenges as more financial activity moves to public blockchain networks:

1. **Privacy:** Ensuring sensitive financial data remains confidential, even as transactions move across institutional and jurisdictional boundaries.
2. **Interoperability:** Enabling different financial platforms and institutions to interact on-chain without sacrificing security, privacy, or compliance.

Select observer list

Anchorage
ANT Group
Avara
Bank of France
Blockdaemon
Citi
Clifford Chance
Commercial Bank of Dubai
Crypto Finance
Deutsche Bank
Deutsche Borse Group
Deutsche Bundesbank
Fidelity International
Fireblocks
Mastercard
Moody's Ratings
Santander
Societe Generale
State Street
Sygnum
Ubyx
UOB Group
U.S. Bank
Wellington Management
Zodia Custody

The primary purpose of the workshop series was to demonstrate ZKsync's Interoperable Prividiums technology for two distinct use cases, identifying how Prividiums may provide enhancements over existing, legacy settlement infrastructures. The prioritized use cases were chosen after consulting with observers from the group. Through live demonstrations, collaborative discussions, and feedback sessions, the working group thoroughly evaluated the practical viability of ZKsync's technology for global, institutional use. This collaborative approach enabled the identification of current limitations of legacy systems, target-state benefits enabled by Prividiums, and potential barriers to adoption, ensuring that the group's collective insights and recommendations were captured in this comprehensive report for the benefit of the broader financial services industry.

Prividium technology: Combining privacy, interoperability, and scalability

Prividium technology introduces distinctive features that deliver measurable advantages across various use cases. By integrating Prividium into workflow processes, these features are enhanced, supporting improved efficiency and effectiveness. The following characteristics illustrate the specific benefits enabled by Prividium technology.

Prividium characteristics:

- **Operational independence:** Each Prividium operates as a fully independent ZK layer 2 network on top of Ethereum, granting complete control to its operator. Institutions can run this technology inside their commonly used infrastructure and can do business as usual, while leveraging the benefits of blockchain technology. They do not need to hold crypto to operate it.
- **Privacy with control:** Prividiums ensure institutional privacy by keeping transaction data off-chain, so internal details such as trade counterparties and balances remain confidential. Off-chain means "off-Ethereum" or thus "off public chain." Instead, transactions are processed on the Prividium by its sequencer and prover and that data is stored by the operator on premises or on cloud (e.g., inaccessible to parties without the required access rights).
- **Built-in compliance:** Prividiums feature role-based access controls and single sign-on integration, as well as support for KYC, know your business (KYB), and AML workflows, as access is gated and only whitelisted accounts can interact with the Prividium blockchain. Compliance checks can be performed as done today and subsequent actions can be taken off-chain, enabling robust compliance capabilities.
- **Ethereum anchoring:** Every batch of transactions is finalized on Ethereum using a validity proof, providing tamper-proof integrity and trust-minimized settlement. By anchoring only proofs to Ethereum, Prividiums leverage the security and auditability of Ethereum's mainnet without exposing sensitive information. Prividiums' operators also have direct access to Ethereum's capital markets, with L1 finality achieved in seconds.
- **Native interoperability:** ZKsync interop provides protocol-level connectivity between chains, which is different from inefficient third-party bridges that either require liquidity on both chains or force creation of a wrapped version of a token. With ZKsync interop any asset or message can be sent over without capital constraints or fragmenting liquidity. Thanks to ZK proof verification and a piece of middleware called ZKsync Gateway, fast, secure and verifiable exchange of assets, data, and execution across private and public ZKsync chains is seamless. This built-in interoperability is unique to ZKsync, delivering cross-chain connectivity without added risk, trust assumptions, or integration overhead.
- **ZK-powered:** At the heart of Prividiums lies ZK proof technology. This makes it possible to anchor transactions to Ethereum for finality and security, while keeping all sensitive business logic and counterparties private. ZK technology also enables trust-minimized collaboration between Prividiums as these ZKsync chains cannot insert malicious transactions. When ZK proofs are posted to the underlying layer, validity is guaranteed and other chains can verify them against Merkle proofs, enabling operators of the chains to transact with each other without trust concerns.

- **Private transaction submission and layer 2 processing:** Users interact with Prividiums through an Remote Procedure Call (RPC) interface, which filters transactions so that only those with explicit permissions or assigned roles can conduct on-chain activities and get access only to data they're allowed to view.
- **Security:** ZKsync takes a multilayered security approach with auditing and review processes starting well before any code is deployed. Always ensuring that all code deployed to production has been thoroughly tested before release, the Matter Labs team conducts internal audits, followed by independent external a udits from reputable auditors and has already spent more than $10 million on audits conducted by top security firms.
- **Customization:** Prividiums are designed for flexibility, allowing enterprises to tailor their deployment to specific operational requirements or use cases without sacrificing trust or interoperability. They can hold multiple assets and can have a custom base token. They don't need to hold/touch any crypto if they don't want to.

As the industry continues to confront persistent inefficiencies and risks inherent to legacy settlement infrastructures, there is a need for transformative solutions that can deliver speed, transparency, and privacy at scale. Prividiums, with their flexible architecture and advanced ZK technology, represent a compelling path forward, offering institutional-grade privacy, operational flexibility, and interoperability required to meet the demands of modern financial markets. To support these benefits, the following sections will delve deeper into the technology underpinning Prividiums, illustrating how these platforms can be deployed to support the in-scope use cases and drive meaningful enhancements to legacy settlement processes. By exploring both the technical foundations and practical applications, we aim to demonstrate how Prividiums can unlock new levels of efficiency, privacy, and trust for business use cases between financial institutions.

"Fireblocks is expanding its support for institutional grade infrastructure by integrating Matter Labs' Prividium, a new enterprise focused permissioned blockchain platform. As financial institutions increasingly adopt permissioned ledgers, this collaboration provides a secure and streamlined pathway to innovation.

Because Prividium is an EVM-compatible platform, Fireblocks clients can seamlessly connect their workspaces to Prividium networks without requiring custom development or altering established user workflows. This native integration allows organizations to leverage Prividium's advanced privacy-preserving and interoperable settlement capabilities while retaining the full security and governance benefits of the Fireblocks platform including its MPC-CMP wallets, policy engine, and granular access controls.

Together, Fireblocks and Prividium deliver a powerful solution, offering institutions the enterprise grade security they require and the next generation blockchain capabilities they seek."

Varun Paul
Senior Director, Financial Markets
Fireblocks

Privacy

Prividiums stand out as the only EVM-equivalent framework currently offering true chain-level privacy, delivering robust privacy by combining secure local processing, tightly controlled access, and advanced cryptographic proofs, ensuring sensitive data remains protected at every stage of the transaction life cycle.

Why anonymity on public chains is not sufficient

1. Pseudonymity ≠ Privacy

- Public chains only offer pseudonymity: Transactions are tied to addresses, not names.
- But in financial markets, transaction metadata itself (size, timing, counterparties) can reveal sensitive business intelligence.
- Once an address is linked to an institution (via KYC at an exchange, on-chain analysis, or leaked data), the entire transaction history is permanently exposed.

2. AI will accelerate de-anonymization

- Advanced AI models are already being trained to correlate wallet activity across chains, exchanges, and external data sources.
- Patterns such as transaction size, timing, counterparty behavior, and even gas usage leave identifiable "fingerprints."
- This means that even if an institution tries to rotate wallets, AI clustering will link them together and unmask participants.
- What looks private today will not be private in one to two years.

3. Multiple transactions reveal trends

- A single transaction might not expose much. But over hundreds or thousands of trades:
  - FX hedging strategies can be reverse engineered.
  - Repo financing patterns can be mapped.
  - Market positions and liquidity stress can be inferred.
- Competitors, counterparties, or even hostile actors can use this to front-run, manipulate, or weaken institutions.

4. L1 privacy is not scalable

- Attempting to hide activity on public L1s with mixers or privacy add-ons introduces:
  - Regulatory risk (mixers are under global scrutiny).
  - Performance bottlenecks—privacy layers slow throughput dramatically.
  - Usability barriers—custom wallets, non-standard APIs, incompatibility with enterprise systems.
- Public L1s simply cannot process millions of private institutional transactions daily at required cost and latency.

"Pseudonymity on a public L1 is a short-lived illusion of privacy—AI analysis will unmask it, and repeated transactions will expose trends. True institutional privacy requires Prividiums."

Alex Gluchowski
Co-founder and CEO of Matter Labs

Why Prividiums solve this

- **Local confidentiality:** All data stays inside the institution's Prividium, never exposed on Ethereum. Only a ZK proof is published.
- **AI-resistant privacy:** Since no raw data leaves the Prividium, there's nothing for AI models to cluster or de-anonymize.
- **Granular visibility:** Institutions can selectively grant regulators full access without exposing anything to competitors or the market.
- **Scalability by design:** Each institution runs its own Prividium at enterprise-grade TPS, but interoperability ensures global settlement.

Institutional privacy by design

By combining a private RPC endpoint and the ability to restrict access to whitelisted accounts and deployments, ZKsync chains can be configured to be both fully private and permissioned.

Key privacy features

- **Off-chain transaction execution and local data storage:** All transactions within Prividium are processed using a local EVM-equivalent engine, ensuring that execution remains entirely within the institution's trusted environment. Data generated from these transactions is securely stored on-premises or in a private PostgreSQL database, managed with familiar enterprise tools and practices. This approach guarantees that sensitive information is kept under the institution's exclusive control, supporting both regulatory compliance and operational security.
- **Private RPC endpoint with granular access controls:** Blockchain interactions are routed through a private SSO-gated RPC endpoint, which serves as a secure gateway for all requests and enforces strict group and role-based access controls. Access is restricted to authorized accounts or roles, such as operations, compliance, and audit teams, ensuring that only those with appropriate permissions can interact with the system to maintain security and privacy. Such requirements can be customized to align with the enterprise's governance rules and policies.

- **ZK proof generation:** After transaction blocks are finalized, Prividium's ZK engine, or prover module, generates cryptographic proofs that attest to the correctness and integrity of all processed transactions. These ZK proofs validate the integrity of transaction execution without revealing any underlying transaction details, inputs, or customer identities, thereby preserving privacy throughout the process.
- **On-chain settlement via proof submission:** For settlement, only cryptographic proofs and root hashes are submitted externally to the Ethereum mainnet, using a lightweight verifier smart contract. This mechanism allows Prividium to achieve on-chain finality while maintaining privacy.
- **Modular processing architecture:** Prividium's architecture is built around several core modules, including a sequencer that aggregates transactions into blocks, a prover that generates ZK proofs, a broadcaster that transmits proofs and transaction details as needed, and an eth sender that publishes proofs and root hashes to external settlement layers. Asset transfers are managed by an escrow smart contract, which atomically burns and mints tokens across chains. The system can also be configured to support lock-and-mint models, providing flexibility to suit various use cases.
- **Protocol-level security and protection:** While unauthorized minting has been a concern on some blockchain networks, Prividiums address this risk by tightly coupling minting and burning actions to valid interoperability transactions, enforced directly by the protocol. This protocol-level enforcement makes unauthorized minting impossible, providing robust protection against such vulnerabilities.

By delivering comprehensive privacy controls, secure local processing, and advanced ZK cryptography, Prividiums set a new standard for institutional confidentiality and regulatory compliance in blockchain-based settlement. These capabilities empower financial institutions to confidently manage sensitive transaction data while maintaining operational flexibility and meeting stringent governance requirements.

Interoperability

Interoperability remains a key capability for institutions seeking to modernize their operations and remain competitive. As markets grow increasingly interconnected both domestically and globally, the ability to efficiently exchange information and assets across disparate systems is a critical requirement. Without robust interoperability, interactions among organizations will remain fragmented, elevate reconciliation costs, and increase settlement risk throughout the transaction life cycle.

"Financial market participants don't want their transaction history published on public chains. Should their wallet address be "doxxed", then their past and future transactions would be open for all to see. Critical transactions like corporate cash management and wholesale financial settlements need to operate on a secure, private, performant substrate. We are moving away from a world of special purpose rails towards the utilization of tokens on general purpose public infrastructures. The cost benefits of doing this are obvious – just think of the special purpose devices that are made redundant by apps on the phone – alarm clocks, calculators, walkmans, etc. For the general purpose technologies to win, they have to meet the needs of financial market participants and privacy, performance and interoperability are high on the risk. We face a paradigm change from silos to multi-asset infrastructures. Only through industry collaboration will we will able to move beyond the one trick pony infrastructures that we use today."

Tony Mclaughlin
CEO, Ubyx

Forget blockchain bridging as we have come to know it. ZKsync's protocol-level interoperability ("interop") is unique and secured by ZK cryptography. It is made possible by smart contracts that verify transactions across chains using Merkle proofs. Another part of the critical infrastructure enabling interop between ZKsync chains is the ZKsync Gateway, which is a hub for ZKsync chains proof aggregation. Gateway enables ZKsync chains to have:

- **Fast interop:** Interchain communication requires quick proof generation and verification. The latter can be very expensive on L1. Gateway provides an L1-like interface for chains, while giving a stable price for compute.
- **Cheaper fees:** Proof aggregation can reduce costs for users, if there are multiple chains settling on top of the same layer.

How it works

Example: One Prividium (the "sending chain") wants to send an asset to another Prividium (the "destination chain"). The process flow depicted in figure 1 explains step-by-step how this is done.

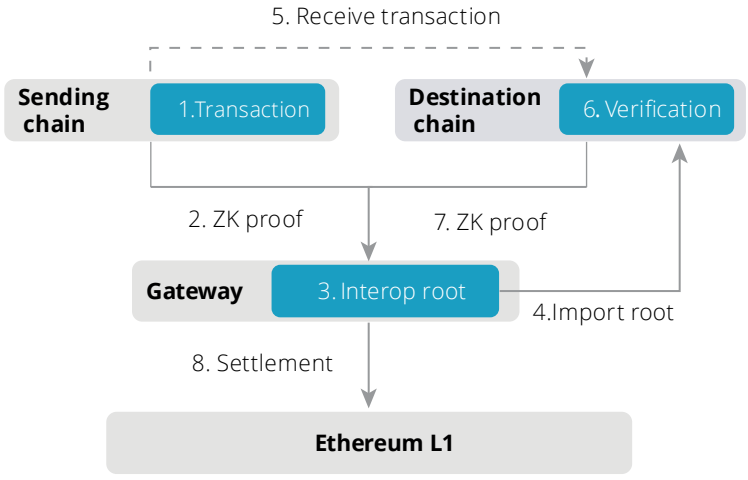
1. Transaction initiation: The sending chain initiates the transaction, including batch and local root data.
2. Proof generation: A ZK proof is generated and sent to the ZKsync Gateway, serving as a cryptographic stamp of integrity for the transaction.
3. Interop root update: The interop root is updated on the ZKsync Gateway, tracking transactions in progress.
4. Import to destination chain: The transaction root is imported to the destination chain, providing context for the incoming transaction.
5. Merkle proof transmission: The broadcaster service transmits the Merkle proof and transaction information from the sending chain to the destination chain.
6. Verification: Upon receipt, the destination chain verifies the Merkle proof against the interop root on the ZKsync Gateway, ensuring transaction integrity.
7. Destination proof generation: The destination chain generates its own ZK proof, confirming that the transactions have been processed.
8. Settlement on Ethereum: By executing transactions off-chain and settling on Ethereum layer 1, Prividiums combine the efficiency and privacy of off-chain processing with the verifiability and security of Ethereum.

This architecture enables enterprises to customize their Prividium environments while maintaining secure, efficient, and trust-minimized interoperability across diverse deployments. Detailed transaction flows for the two use cases explored will show various models to which Prividiums can be applied.

"Interoperability isn't an add-on. It's in the DNA of ZKsync."

Yuliya Alexiev
VP of Product, Matter Labs

Figure 1. Prividium interoperability process flow



Performance and cost benchmarks

High-performance and scalability

While Prividiums are able to provide institutional-grade privacy and interoperability among Prividiums, they are also engineered for performance and scalability, leveraging advanced cryptographic and system optimizations to deliver enterprise-grade throughput and efficiency.

Powered by ZKsync's new open-sourced prover, AirBender, the fastest RISC-V zKVM, and in coordination with its enhanced sequencer and database architecture, Prividiums are capable of supporting massive transaction volumes with minimal latency and cost when AirBender and database optimizations are in place.

Key performance metrics achieved with AirBender are:

- **Throughput:** Achieve up to 10,000 TPS, enabling high-volume applications and large-scale enterprise deployments. Horizontal scaling can occur as multiple Prividiums are spun up (each processing 10,000 TPS), implemented, and connected in parallel, enabling unlimited throughput for enterprises, just like we spin up more servers to scale the internet. This is again enabled by ZK proof technology as multiple ZK proofs can be aggregated into one equally secure ZK proof to be posted to Ethereum.
- **Cost:** Proving costs are less than $0.0001 per transaction, making it economical to operate at a significant scale.
- **Low latency:** Block times are consistently in the 100–200 millisecond range, supporting near real-time transaction finality.
- **Low overhead:** Level of performance is attainable on commodity hardware, reducing the operational burden and making it feasible to run large private blockchains at low cost.
- **Speed:** Delivers sub-second proofs for ZKsync blocks and approximately 3-second proofs using a single commodity GPU.
- **Efficiency:** Four to six times faster than the closest competing systems.
- **Resource optimization:** Proves Ethereum blocks in under 35 seconds using just one GPU, compared to other setups that require 50–160 GPUs to achieve 12-second proofs (depending on block size).
- **Decentralized potential:** Developers can build client-side applications that generate proofs locally, contributing to a faster, more cost-effective, and increasingly decentralized ecosystem.

Through these innovations, ZKsync Prividiums are setting a new standard for high performance and scalability in private blockchain environments, empowering enterprises to operate at scale without sacrificing efficiency or cost-effectiveness.

Cost analysis

As ZKsync technology has matured, the cost of proving and settling transactions has declined rapidly, making Prividium deployments increasingly cost-effective. Ongoing advancements in ZKsync's infrastructure have driven significant reductions in per-transaction costs, positioning Prividium as a highly competitive solution for enterprise blockchain operations.

Rapid decline in proving costs

From 2023 to 2025, ZKsync technology has consistently driven down per-transaction proving costs, culminating in the introduction of Airbender, the latest and most cost-efficient proving solution to date. Transactions refer to a single, individual operation processed on the ZKsync Prividium blockchain.

- 2023 (Boojum): ~$0.05 per transaction
- 2024 (Optimized Boojum): ~$0.001 per transaction
- 2025 (Airbender): ~$0.0001 per transaction (10x cheaper than Optimized Boojum)

The dramatic reduction in proving and settlement costs underscores Prividium's evolution into a highly scalable and economically viable solution for enterprise blockchain adoption. As ZKsync technology continues to advance, most notably with the introduction of Airbender, institutions can now process transactions at a fraction of previous costs, enabling broader use cases and greater operational efficiency.

Fee predictability

One of the key differentiators of Prividiums compared to public L1s is predictable, low-cost settlement fees. On general-purpose public blockchains like Ethereum, transaction costs are highly volatile. Gas prices fluctuate depending on network congestion, meaning the same transaction can cost pennies one moment and dollars the next. For institutions processing millions of transactions daily, this lack of predictability creates significant operational and accounting challenges.

Prividiums solve this through a combination of ZK proof aggregation and the ZKsync Gateway:

- **Proof aggregation:** Instead of settling each transaction individually, thousands of transactions are compressed into a single ZK proof. This amortizes settlement costs across many transactions, driving proving costs down to less than $0.0001 per transaction.
- **Stable pricing:** The enterprise running its Prividium can choose when and how often to close batches and post proofs to Gateway, effectively controlling its costs. Institutions can plan around consistent pricing models, rather than being exposed to fee spikes.
- **Institutional forecasting:** This stability allows treasurers, operations teams, and financial controllers to accurately forecast costs and integrate blockchain settlement into enterprise P&L models without risk of cost blowouts.

Use cases

Prividiums are designed to support any institutional use case. To showcase their capabilities in practice, two of the most complex and widely recognized transaction types in global finance were selected after consulting with a number of the workshop participants: cross-border payments and intraday repurchase agreements (repos).

These use cases were chosen for three reasons:

1. **High impact:** They represent some of the largest transaction volumes in financial markets.
2. **Clear inefficiencies:** Both processes today are slow, fragmented, and costly.
3. **Strict privacy requirements:** Sensitive counterparty and balance data cannot be exposed.

By tackling these "hard cases," Prividiums demonstrate their ability to deliver speed, efficiency, cost reduction, and privacy where it matters most.

For each use case, the group began with a review of today's workflows, identified the main risks and limitations, and then mapped alternative on-chain architectures. From this analysis, a target-state architecture was selected and demonstrated live, highlighting how Prividiums address the shortcomings of current systems.

Use case 1: Cross-border payments

Cross-border payments today are built on a complex web of correspondent banking relationships. This traditional model requires financial institutions to maintain pre-funded nostro and vostro accounts across multiple jurisdictions, resulting in significant operational complexity. These arrangements expose institutions to a range of risks, including settlement, credit, and reconciliation challenges, and often lead to inefficient use of capital due to liquidity being locked up in fragmented accounts.

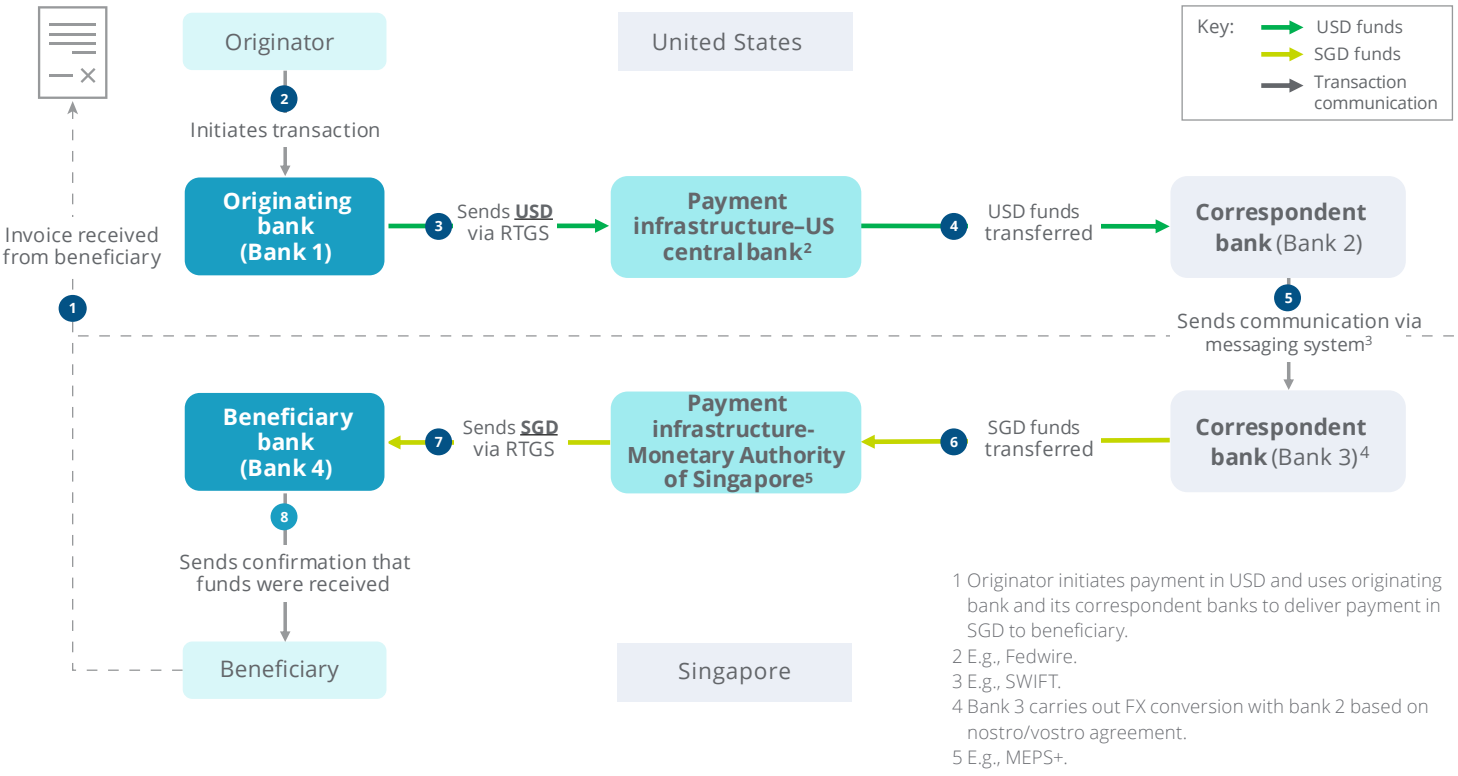
Today's problem:

- Pre-funded nostro and vostro accounts immobilize approximately $27 trillion.
- Settlement can take up to 3–5 days with multiple intermediaries.
- Corporates pay an estimated $120 billion in fees annually, excluding FX costs.

With Prividiums:

- Near-instant settlement across interoperable bank blockchains.
- Liquidity consolidated at an FMI chain (one of the many architecture options), eliminating idle capital.
- End-to-end privacy, with only proofs shared to Ethereum.
- Costs significantly reduced by cutting out correspondent banks.

Figure 2. Current-state cross-border payment through correspondent relationship (USD – SGD)



1 Originator initiates payment in USD and uses originating bank and its correspondent banks to deliver payment in SGD to beneficiary.
2 E.g., Fedwire.
3 E.g., SWIFT.
4 Bank 3 carries out FX conversion with bank 2 based on nostro/vostro agreement.
5 E.g., MEPS+.

Current cross-border payments transaction flows

As depicted in figure 2, numerous intermediaries and varying legal jurisdictions are involved throughout a cross-border payment transaction. Notably, four distinct banks alongside central banks in this case are engaged in the orchestration and instruction of these payments, underscoring the operational complexities and challenges inherent in today's systems. The typical transaction flow is as follows:

1. The beneficiary issues an invoice to the originator.
2. The originator initiates payment through its primary financial institution (Bank 1).
3. Funds are processed via the US central bank, utilizing RTGS or Fedwire systems.
4. The payment is subsequently routed to the correspondent institution (Bank 2).
5. Correspondent banks coordinate across jurisdictions, facilitating the transfer of funds to the beneficiary's bank via messaging system such as SWIFT.
6. Correspondent bank (Bank 3) converts USD to SGD with correspondent Bank 2 based on nostro/vostro agreement and sends SGD to a payment infrastructure (Monetary Authority of Singapore) for further processing.
7. Beneficiary bank (Bank 4) receives SGD from payment infrastructure via RTGS.
8. Beneficiary bank (Bank 4) sends confirmation to the beneficiary that the funds were received.

Current-state risks and challenges of cross-border transactions

In the current landscape of cross-border payments, several persistent challenges and operational inefficiencies are apparent. These issues are exacerbated by the multi-jurisdictional nature of such transactions, which typically require coordination among multiple financial institutions, regulatory regimes, payment infrastructures, and operating hour limitations. The following outlines the primary obstacles and risks faced in today's cross-border payments environment:

- **Slow and uncertain settlement times:** Cross-border payments remain markedly slower and less predictable than domestic transfers. Cross-border payments settlement times typically take one to five business days to settle, whereas most domestic payments clear the same day.[1]
- **Idle and fragmented capital:** To facilitate international transactions, banks must pre-fund numerous nostro accounts across various jurisdictions, leading to substantial amounts of idle capital. It was reported that an estimated $27 trillion is locked in pre-funded nostro and vostro accounts, highlighting the vast scale of funds immobilized in the current system.[2] This not only reduces liquidity available for other business activities but also limits financial flexibility.
- **Limited visibility and costly reconciliation:** The lack of real-time transaction tracking and standardized data formats makes it difficult for institutions to monitor payment status and balances. As a result, reconciliation can take weeks and cost up to 10 times more than domestic transactions, driving up operational expenses and increasing the risk of errors or disputes.[3]
- **Stacked intermediary fees:** The involvement of multiple correspondent banks in cross-border payments leads to a compounding of fees at each step. Corporations move approximately $23.5 trillion across borders annually, incurring an estimated $120 billion in transaction fees each year, excluding foreign exchange costs.[4]
- **Systemic and counterparty risk:** Beyond individual transaction challenges, the cumulative complexity of cross-border payment networks introduces systemic vulnerabilities. The reliance on multiple intermediaries and jurisdictions increases the likelihood that disruptions, errors, or insolvencies at any point in the chain can cascade, impacting multiple parties. This interconnectedness exposes institutions to counterparty risk and can undermine trust in the global payments infrastructure, especially during periods of market stress or volatility. This risk environment has contributed to a 22% reduction in the number of active correspondent banks worldwide between 2011 and 2019, concentrating transaction volumes among fewer institutions and potentially heightening systemic vulnerabilities.[5]

Target-state overview and process flows

By integrating Prividiums into a variant of on-chain cross-border payments, the technology demonstrates its potential to address many of the persistent challenges facing today's cross-border payments landscape. While this process flow is not the only architecture that can be deployed through Prividiums for cross-border payments, this specific use case is based on the below architecture assumptions:

- **Three-chain model and stablecoin provisioning:** Demonstration was based on a three-chain architecture, where each participating bank issues its own stablecoin (USD and SGD respectively) and operates its own Prividium, and a dedicated FMI liquidity app chain coordinating FX, clearing, and settlement.
- **Stablecoins:** It is assumed that stablecoins are used here for the transfer. In practice, tokenized deposits or other forms of digital assets can also be used.
- **FMI liquidity reserves:** FMI maintains sufficient reserves in both domestic and foreign stablecoins to facilitate settlement.

- **Invoice-led payment flow:** The scenario presumes that a corporate client of the beneficiary bank issues an invoice in its local currency (SGD) to a payer at the originating bank in the US.
- **FX rate sourcing:** The FMI is assumed to provide near real-time FX quotes, leveraging oracles that are connected to live FX market data.
- **Compliance screening:** Both transacting parties are assumed to have completed their respective compliance screenings prior to initiating the transaction. In a production environment, integrations with KYC/AML solutions such as Elliptic, Chainalysis, or similar providers would be possible. Additionally, Travel Rule data exchange is assumed to occur via networks like Notabene or Coinbase TRUST, though other integrations could be supported.
- **Wallet infrastructure:** For demonstration purposes, MetaMask is used as the wallet infrastructure. In a production setting, the architecture is designed to support a range of institutional wallet providers, such as Blockdaemon, Fireblocks, or any other corporate-preferred solution.

These foundational assumptions are intended to navigate the use case to highlight the core capabilities of the proposed architecture, while acknowledging that certain operational, regulatory, and technical considerations would need to be addressed for real-world deployment.

"As financial institutions advance toward interoperable, privacy-preserving infrastructure, platforms like ZKsync Prividiums demonstrate that privacy and compliance are complementary, not conflicting, priorities. These capabilities are essential for blockchain to become part of the fabric of the global financial system.
To scale effectively, next-generation infrastructures must support real-time compliance and risk visibility—safeguarding institutional integrity without compromising on speed, privacy, or performance. Prividium's architecture, embedding role-based access, auditability, and zero-knowledge proofs, sets a new standard for secure and compliant settlement.

To support widespread adoption, financial institutions will also require end-to-end transaction intelligence across assets, networks, and protocols. This is where Elliptic plays a key role—delivering the breadth, depth, and real-time insights necessary to identify and mitigate emerging risks. Together, solutions like Prividium and Elliptic enable trusted, scalable, and compliant infrastructures for the next era of finance."

Andrea Camacho
Principal Product Manager, Elliptic

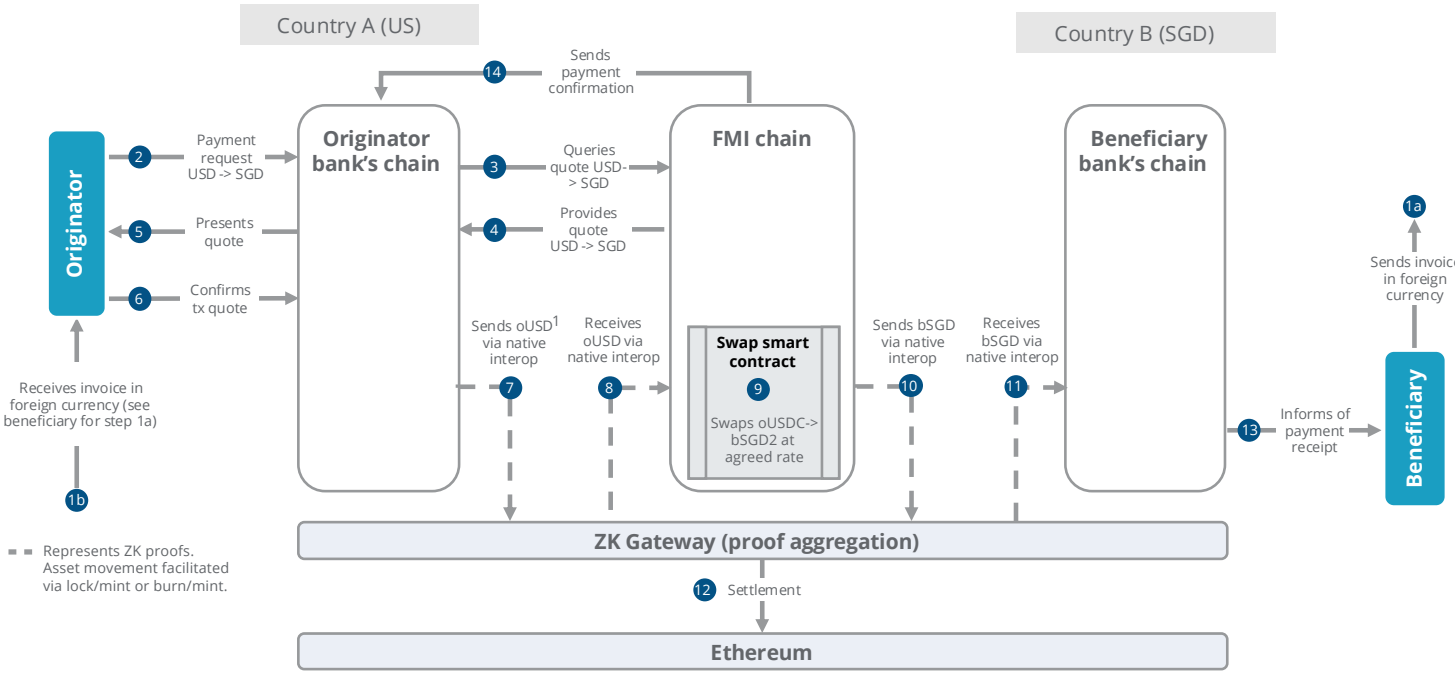
Target-state process steps

Cross-border payment architecture: Sequential steps in the demo

1. **Invoice display:**
   a. The demo begins with the display of invoice terms sent by a client of the beneficiary bank "b" in Singapore to a client of originator bank "o" in the US. The invoice requests payment to the beneficiary's account in Singapore dollars.
   b. Originator bank receives an invoice in foreign currency.
2. **Originator portal interaction:** The client of the originator bank logs into its portal and inputs the payment terms.
3. **FX quote request:** The originator bank queries a quote from the FMI liquidity appchain.
4. **Quote display and client confirmation:** FMI chain provides the requested quote. Once the quote is received, it is displayed on the sending client's portal. The client reviews and confirms the payment.
5. **Interoperable transaction initiation:** Quote is displayed on the sending client's portal.
6. **Quote confirmation:** The client reviews and confirms the payment.
7. **Initiate transaction:** Upon confirmation, the originator bank chain initiates an interop transaction sending USD. A ZK proof is sent to the gateway, which the FMI chain can verify.
8. **FMI chain receives USD:** FMI chain receives ZK proof via native interoperability.
9. **Asset transfer mechanism:** The actual asset transfer is facilitated via "lock and mint" or "burn and mint" mechanisms, depending on the preference of the Prividiums. Both options are available for native and bridged Prividium assets. The asset pair is automatically swapped at the agreed rate within a smart contract, using pre-funded liquidity.
10. **FX swap execution:** Post-execution of swap, FMI chain initiates interop transaction and sends SGD to the beneficiary bank.
11. **Beneficiary bank receives SGD:** Beneficiary bank receives SGD sent from FMI chain via native interoperability.
12. **Settlement:** An aggregated proof is settled on Ethereum.
13. **Notification:** The beneficiary is notified of payment receipt.
14. **Payment confirmation:** The originator receives confirmation from the intermediary chain, concluding the transaction.

While this process flow may appear more complex, it is designed to provide a detailed depiction of each step. In practice, most steps will be automated, resulting in faster, more efficient transactions with reduced risk, in comparison to today's settlement infrastructures.

Figure 3. Cross-border payment target-state flow



1 oUSD represents originator bank USD stablecoin.
2 bSGD represents beneficiary bank SGD stablecoin.

Target-state benefits with interoperable Prividiums

- **Native interoperability across institutions**
  - Each bank operates its own Prividium, configured for its compliance and governance needs, yet transactions flow seamlessly across chains. Prividiums interconnect without congestion or fee volatility.
- **Liquidity without nostros, lower costs through fewer intermediaries**
  - Direct chain-to-chain settlement reduces reliance on multiple correspondent banks.
  - The architecture choice to add one intermediary chain holding liquidity is by choice, but with this particular architecture, the FMI chain maintains shared liquidity pools, decreasing the need for banks to pre-fund accounts. This model does not completely eliminate the need to maintain liquidity, but does provide the ability to reduce the amount of liquidity needed to be placed in different nostro accounts.
  - With fewer fees stacked into each payment, costs drop dramatically.
- **Speed**
  - All these steps depicted in figure 3 happen in a matter of minutes.
- **End-to-end privacy with compliance**
  - Transaction details (amounts, counterparties, balances) remain private within each bank's Prividium.
  - Only employees with the right credentials can view or access.
  - Regulators can receive data on request.
  - No sensitive business logic or strategy is ever exposed on-chain.
- **Atomic FX + settlement**
  - Interop ensures FX conversion and payment legs clear together, across chains, eliminating settlement risk.
- **Scalable architecture**
  - Each bank can scale independently and deploy multiple use cases by running its own Prividium without bottlenecking others — something impossible on a single shared ledger.
- **Near real-time finality, 24/7**
  - Payments settle in seconds, around the clock, including weekends and holidays.
  - This aligns with growing expectations for always-on financial services.
- **Closer to today's workflows, but modernized**
  - The client still logs into their bank portal, requests an FX quote, confirms payment, and receives confirmation.
  - What changes is what happens behind the scenes: Blockchain-based automation ensures privacy, interoperability, and atomicity.
  - This minimizes the integration gap for institutions while delivering the full benefits of next-generation infrastructure.

The Prividium target state retains the familiar structure of today's cross-border payment workflows, invoices, bank portals, FX quotes, and compliance checks, but it removes the operational friction that slows settlement and ties up liquidity. Instead of reengineering how banks interact with their clients, Prividiums streamline the processes behind the scenes, using ZK proofs and interoperability to achieve speed, privacy, and security.

"Prividium operators can integrate Blockdaemon's secure infrastructure to streamline wallet management and chain operations. During setup, Prividium issues a unique API key for Blockdaemon's MPC wallet services, automating the user registration process. MPC wallets function as isolated groups within Prividium and provide blockchain data for managed users through efficient API calls. This simplifies access control by allowing operators to manage permissions from a single MPC wallet admin panel while maintaining compliance and security."

Brad Turner
Director of Product, Blockdaemon

Operational considerations

Implementing Prividiums in the financial sector demands attention to several foundational areas, each critical for regulatory compliance, system efficiency, risk management, and institutional adoption.

Regulatory alignment and FMI licensing

- **Fragmented regulation:** Stablecoins and other digital assets face inconsistent treatment across jurisdictions, impacting their use for settlement and payments. Some regions classify stablecoins as e-money, securities, or payment tokens, affecting their legal status and utility.[6]
- **FMI licensing:** The solution must operate under the oversight of a licensed FMI, either by integrating with an existing FMI to host the appchain or by establishing a new FMI entity for this purpose.

Governance, operating model, and liquidity pools

- **Governance gaps:** An established and comprehensive governance framework is critical for effective oversight of Prividium, encompassing formal mechanisms for voting, risk management, and system upgrade protocols. Sixty-eight percent of institutional investors identified lack of clear governance as a major impediment to digital asset investment.[7]
- **Liquidity fragmentation:** Institutions are hesitant to commit capital without strong operational models. Liquidity fragmentation remains a persistent challenge, limiting network scale, utility, and broader adoption.[8]
- **Onboarding and incentives:** Effective onboarding and incentives are critical for banks to seed and maintain multicurrency liquidity pools, supporting efficient settlement and FX operations.

Risk and controls

- **Oracle manipulation:** FX pricing oracles must aggregate data from multiple sources and implement fallback logic. In 2024, oracle exploits alone caused more than $53 million in losses across at least eight incidents.[9]
- **Compliance enforcement:** Comprehensive configuration of KYC/AML processes, sanctions screening, and Travel Rule data exchange should be implemented across all participating entities. As of early 2024, nearly one-third of jurisdictions had not yet implemented the FATF Travel Rule,[10] and global financial institutions faced $6.6 billion in penalties for AML/KYC noncompliance in 2023.

Institutional enablement

- **Integration complexity:** Onboarding of originator and beneficiary banks is vital, requiring secure wallet provisioning, smart-contract permissioning, and robust credentialing. Blockchain integration with legacy systems remains a significant hurdle.[12]
- **Market growth:** With the institutional digital asset market projected to exceed $10 trillion by 2030,[13] demand for secure, compliant onboarding will only increase.

"The emergence of frameworks like ZKsync Prividium, which leverage zero-knowledge cryptography to enable programmable privacy, signals a maturing ecosystem that is beginning to address the complex requirements of regulated environments. Evaluating Prividium alongside other industry experts underscores how combining zero-knowledge techniques with verifiable access controls could support both confidentiality and institutional auditability, a necessary balance for real-world financial systems operating at scale. With the Mastercard Multi-Token Network (MTN), we have intentionally designed for complementarity and interoperability across diverse blockchain environments. This includes supporting networks built with Prividium stack, while ensuring that transactions remain programmable, traceable, and compliant with institutional requirements."

Soumyajit Mitra
Director Product Management - Technical
Mastercard

Use case 2: Intraday repo

Today's problem:

- Complex web of custodians and cutoff times.
- Manual reconciliation could lead to settlement delays and collateral lockup.
- High daylight credit risk.

With Prividiums:

- Smart-contract-based atomic settlement of cash and collateral.
- 24/7 liquidity, unconstrained by market hours.
- Reduced operational risk and enhanced capital efficiency.
- End-to-end privacy, with only proofs shared to Ethereum.

A USD repo operates as a short-term secured sale and repurchase agreement, providing a flexible financing tool for institutions. In this arrangement, one party sells an asset, such as US Treasury securities, to another party at an agreed-upon price, with a commitment to repurchase the same securities at a predetermined price in the future. The securities serve as collateral, safeguarding the lender's position.

The repo market plays a vital role in the financial industry by offering two primary benefits: It enables institutions with short-term liquidity needs to access low-cost funding, while allowing those with excess cash to earn a secure return by investing in high-quality, liquid assets.

USD repo transactions are typically structured in two main ways:

1. **Bilateral USD repo:**
   In this model, the cash provider (lender) and the cash borrower (collateral provider) interact directly, without involving a tri-party intermediary. This approach is often chosen when specific collateral types are required or when participants prefer direct negotiation and settlement.
2. **Tri-party USD repo:**
   In this structure, the cash provider and cash borrower engage through a central counterparty (CCP), a custody bank, or both. Utilizing these intermediaries enhances risk management and operational efficiency throughout the transaction process.

Both bilateral and tri-party USD repo transactions can be executed onshore (within the US) or offshore (outside the US), offering flexibility to meet the diverse needs of market participants.

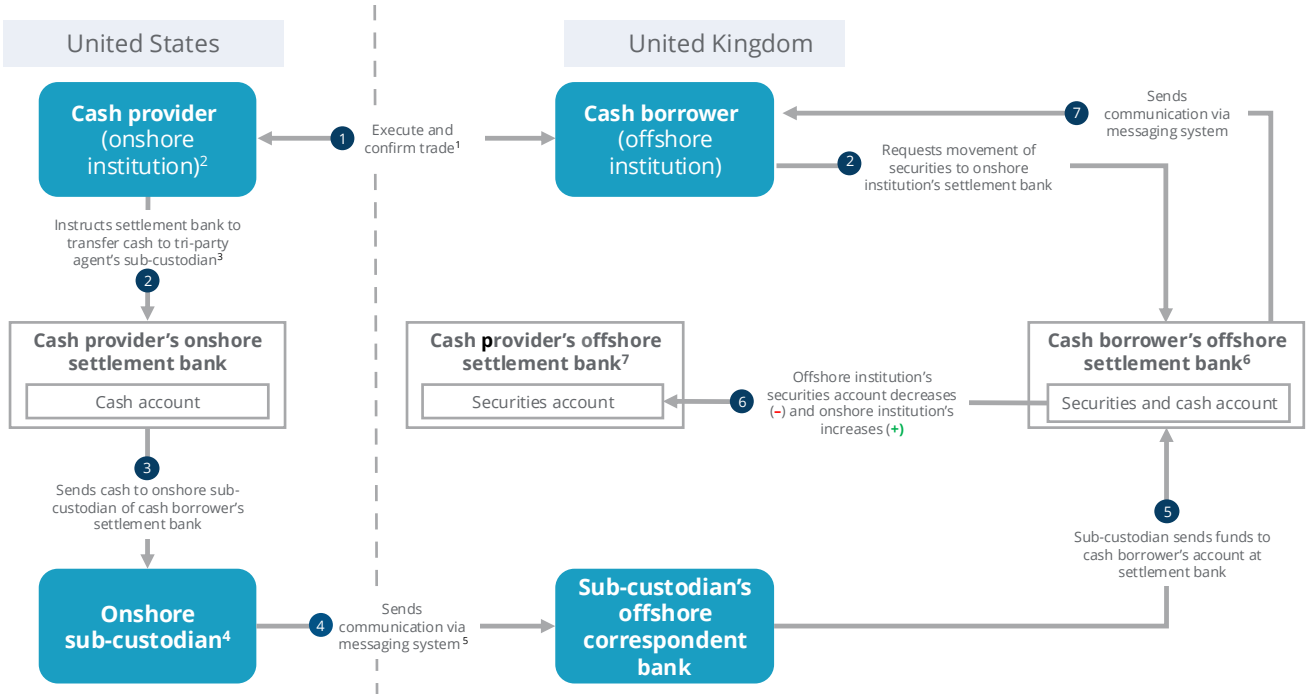
Current USD repo transaction flows

Offshore bilateral USD repo
Offshore bilateral USD repo transactions are short-term secured lending arrangements conducted outside the United States and denominated in US dollars. These transactions do not involve a central counterparty. Offshore bilateral repos are commonly utilized by institutions based outside the US to obtain short-term funding and efficiently manage their liquidity in US dollars. This approach enables international participants to access USD financing while still leveraging high-quality collateral and maintaining flexibility in their funding operations.

Offshore (non-centrally cleared) bilateral intraday repo assumptions

- Multiple market deadlines apply, dependent on the requirements of each local foreign market.
- The onshore cash provider communicates with the offshore clearing and custody bank regarding the delivery of funds.
- The US cash provider does not already maintain funds at its offshore settlement bank.
- Onshore sub-custodian can directly utilize an affiliate bank in the UK, where funds are already held, without the need to engage a correspondent bank in the US.
- Refers to the use of SWIFT for messaging and settlement.
- Cash borrower already holds the relevant securities at the UK clearing or custody bank.
- After encumbrance, the cash provider's offshore settlement banks would notify the onshore institution of successful segregation.

Figure 4. Offshore (non-centrally cleared) bilateral intraday repo process



1 Multiple market deadlines, dependent on local foreign market.
2 Onshore cash provider communicates with offshore clearing and custody bank that funds will be delivered.
3 Assumes the US cash provider does not already have funds at its offshore settlement bank.
4 Assumes the onshore sub-custodian does not need to utilize a correspondent bank in the US and can directly utilize an affiliate bank in the UK where it already holds funds.
5 I.e., SWIFT.
6 Assumes the cash borrower already has securities at the UK clearing/custody bank.
7 After encumbrance, the cash provider's offshore settlement banks would send a notification to the onshore Institution of successful segregation.

Current offshore (non-centrally cleared) bilateral intraday repo process flow:

1. **Execution and confirmation:** Cash provider (onshore institution) in Country A (US) executes and confirms the trade with the cash borrower (offshore institution) in Country B (UK).
2. **Instruction to settlement bank:** Cash provider instructs its onshore settlement bank to transfer cash to its settlement bank.
3. **Cash transfer:** Onshore settlement bank sends cash to the onshore sub-custodian of the cash borrower's settlement bank.
4. **Communication via messaging system:** Onshore sub-custodian sends communication to the sub-custodian's offshore correspondent bank using a messaging system.
5. **Fund transfer to cash borrower:** Sub-custodian sends funds to the cash borrower's account at its offshore settlement bank.
6. **Securities movement:** Cash provider's offshore settlement bank records a decrease in the offshore institution's securities account and an increase in the onshore institution's securities account.
7. **Final communication:** Cash borrower sends communication via a messaging system to confirm the movement of securities to the onshore institution's settlement bank.

Current-state risks and challenges

When analyzing offshore intraday USD repo transactions, specifically offshore non-centrally cleared bilateral USD repo and offshore tri-party USD repo, several risks and operational challenges emerge. These challenges are particularly acute due to the cross-jurisdictional nature of these transactions, which typically involve one US entity and one non-US entity exchanging USD cash for securities.

- **Complex regulatory landscape:** Varying reporting requirements and oversight by different regulators create compliance complexity and oversight gaps for intraday repo transactions, as no standardized process exists for multi-jurisdictional reporting. Recent surveys show that 75% of compliance leaders in Europe's financial sector report rising regulatory demands, intensifying operational strain on compliance teams.[14] For firms operating in multiple markets, this lack of harmonization not only increases compliance costs but also elevates overall risk exposure.
- **Time zone and jurisdictional limitations:** Differences in market hours and time zones, combined with limited operating windows of central bank payment systems, narrow the periods during which liquidity and collateral can move for intraday repo transactions. These jurisdictional and system constraints create operational bottlenecks, delay the timely settlement of assets across markets, and elevate both liquidity and settlement risk. Although up to 90% of US Treasury delivery versus payment (DVP) repos settle by midday, market participants continue to rely on overnight structures not out of preference but because fragmented settlement windows restrict the flexibility required to manage intraday funding needs efficiently.[15]
- **Settlement delays and collateral lockup:** Settlement delays, early cutoff times, and collateral lockup, often worsened by manual processing, impede liquidity management for intraday repo transactions by limiting the timely reuse of cash and securities. These inefficiencies can reduce operating margins for medium-size firms by up to 15%, as they are compelled to rely on costly overdrafts or short-term loans to bridge intraday funding gaps. This direct link between settlement inefficiency and increased funding costs highlights the need for more streamlined and automated settlement processes.[16]

Target-state overview and process flows

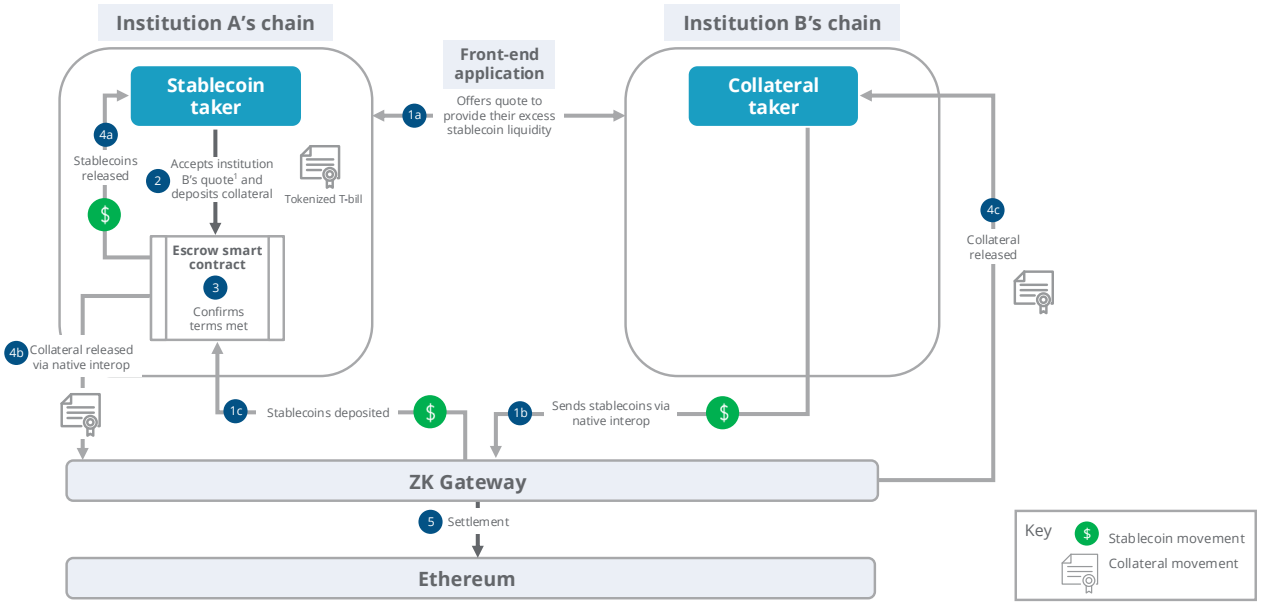
The target state for the bilateral intraday repo use case leveraged an architecture that connects multiple financial institutions directly on-chain, enabling each participant to issue and manage tokenized collateral and stablecoins. In the instance of a tri-party flow, which was not tested as a part of this exercise, an FMI chain could be able to orchestrate the atomic settlement between transacting parties, whereas bilateral transactions are able to be settled directly between trade counterparties. While the configuration outlined in figure 5 serves as the basis for this analysis, Prividium's customizable architecture offers institutions the flexibility to tailor deployment and usage to a wide range of use cases and operational preferences.

Prividium bilateral intraday repo

To effectively illustrate the technological capabilities of Prividiums, the following foundational assumptions have been established for this use case:

- Institution A operates as the stablecoin taker.
- Institution B serves as the collateral taker.
- The marketplace infrastructure is deployed on institution A's blockchain network.
- Marketplace quotes are configurable, enabling customization of parameters such as duration, interest rate, and collateral requirements.
- The escrow smart contract is implemented on institution A's blockchain.

Figure 5. Prividium bilateral intraday repo flow



1 Quote visible in front-end application.

Prividium bilateral intraday repo flow steps:

1. a. Institution B (collateral taker) offers quote to provide its excess stablecoin liquidity.
   b. Institution B (collateral taker) sends stablecoins via native interop to the escrow smart contract.
   c. Stablecoin is deposited into the escrow smart contract.
2. Institution A (stablecoin taker) accepts institution B's offer and deposits collateral into the escrow smart contract.
3. The smart contract verifies that the terms of the trade are met.
4. a. After verification is confirmed, the contract atomically releases stablecoins to institution A.
   b. Collateral is released via native interop.
   c. Once released via native interop, collateral is received by institution B.
5. Entire flow is settled on Ethereum via ZK proof.

Target-state benefits with interoperable Prividiums

- **Atomic cross-chain repo settlement:** Settlement risk is mitigated through the use of escrow smart contracts, which ensures atomic settlement of both transaction legs. This mechanism guarantees that transactions are either fully completed or not executed at all, eliminating timing mismatches and obviating the need for third-party credit lines to cover settlement gaps.
- **Automation:** Automated execution via smart contracts orchestrates both the initiation and completion of repo transactions. This end-to-end automation removes manual interventions and reconciliation steps, accelerating settlement cycles, and enhancing capital efficiency and operational efficiency for participating institutions.[17]
- **Privacy-preserving collateral management:** Repo terms, collateral positions, and counterparties remain confidential to each institution while still seamlessly interoperating for settlement.

- **24/7 interoperable liquidity:** Repo transactions can be conducted across time zones and market hours, with multiple institutions' Prividiums linked together. The Prividium platform delivers continuous, 24/7 liquidity access. By removing the temporal limitations of traditional financial infrastructure, the system enables bilateral and tri-party repo transactions to settle at any time, including outside standard market hours, on weekends, and during holidays, unlocking intraday liquidity that would otherwise remain inaccessible.
- **Regulatory alignment per institution:** Each institution can apply its own compliance workflows (AML/KYC, reporting, regulator nodes) to its Prividium, while still participating in global repo settlement. Prividium's role-based access control allows institutions to grant secure, permissioned access to supervisors and regulators, consolidating activity through a single channel. By enabling increased control and transparency, Prividiums streamline compliance processes and enhance the effectiveness of regulatory reporting and oversight. On shared ledgers, uniform compliance standards are almost impossible to enforce across all actors.
- **Resiliency and control:** A single sequencer, controlled by an institution, is sufficient to ensure security of the setup. Multi-operator setups (e.g., bank and regulator, or consortium banks) are possible, too, to ensure redundancy and resilience while still interoperating with other Prividiums.

Overall, the target-state architecture for intraday repo transactions enables faster, more cost-effective, and highly auditable repo transactions, while reducing operational risk and unlocking continuous liquidity for financial institutions.
Prividium technology introduces a viable solution to address the current industry challenges associated with repo transactions. By leveraging advanced ZK proofs and smart contract automation, Prividiums deliver enhanced transparency, operational efficiency, privacy, and continuous liquidity, addressing long-standing pain points in the repo market.

Operational considerations

Implementing Prividiums requires addressing several foundational operational areas. Each is essential for regulatory compliance, system efficiency, risk management, and institutional adoption.

Cash leg challenges

- **Stablecoin classification and utility:** At the time of writing, stablecoins are still not recognized as "cash equivalents" under US GAAP, MMF, or LCR frameworks, restricting their use for intraday liquidity and daylight overdraft management at central banks. When treated as crypto exposure, they trigger additional counterparty-credit and market-risk capital requirements, increasing operational complexity and costs. It is important to note that the GENIUS Act does introduce the possibility for stablecoins issued by a permitted payment stablecoin issuer, or PPSI, to be classified as cash equivalents, but further industry alignment is still required.
- **Regulatory shifts:** It is important to continuously monitor and adapt to regulatory changes, such as the Basel Committee on Banking Supervision (BCBS) finalizing stricter stablecoin criteria in July 2024. These new requirements, which emphasize reserve asset quality and liquidity, are scheduled for implementation in January 2026.[18]

Collateral eligibility gaps

- Legal and operational uncertainty: Digital collateral ownership hinges on private key control, diverging from traditional legal contracts, especially across jurisdictions. CCP and tri-party rulebooks reference the CUSIP/ISIN of the underlying security, not its tokenized form, leaving margin-model haircuts and value-added reseller (VAR) add-ons for tokenized assets undefined or inconsistent across the industry.

Transfer agent and asset servicing constraints

- **Operational disconnects:** Blockchain enables 24/7 token movement, but registrars and transfer agents for underlying assets operate during standard business hours, risking stranded collateral if corporate actions occur outside those windows. Similar limitations affect Fedwire Securities and DTC, meaning tokenized assets may not always achieve "T+0 finality."
- **Settlement cycle modernization:** While blockchain technology offers the potential for near-instantaneous (T+0) settlement, fully realizing these benefits across the financial ecosystem would require the broader market to further accelerate its settlement cycle beyond current standards. The recent transition to T+1 in US securities markets is a step forward, but additional modernization would be necessary to support true real-time settlement and unlock the full efficiency gains blockchain can provide.

Capital and balance sheet treatment

- **Unclear capital treatment:** No standardized approach exists for capital treatment of tokenized assets. Permissionless networks face punitive risk weights (Group 2 at 1,250%), while permissioned networks may qualify for lower weights (Group 1 at 100%) under Basel III Endgame, significantly impacting capital requirements.[19]
- **Netting set fragmentation:** Tokenized repos may not offset against traditional repo books, complicating leverage ratio and global systemically important bank (GSIB) surcharge calculations.

Jurisdictional and cross-border friction

- **Legal variability:** Title transfer, close-out netting, and insolvency treatment differ widely across jurisdictions, meaning finality in one region may not be recognized elsewhere.
- **Compliance challenges:** Divergent AML and KYC standards on factors such as on-chain identity disclosure may impede bilateral and tri-party trades. By 2025, 92% of centralized crypto exchanges globally are fully KYC compliant (up from 85% in 2024), though overall market-wide compliance is 79%.[20]

Connecting to blockchains outside the ZKsync ecosystem

- It's possible to connect to non-Ethereum, non-ZKsync chains with third-party bridges. ZKsync integrated Axelar, LayerZero, Chainlink Cross-Chain Interoperability Protocol (CCIP), and Across.
- Institutions adopting Prividium technology should do their own due diligence when selecting a bridge provider.

The current intraday USD repo market is characterized by complex, multi-jurisdictional workflows and persistent operational challenges, including settlement delays, regulatory fragmentation, and heightened liquidity risk. These inefficiencies not only constrain institutions' ability to manage short-term funding but also elevate compliance and operational costs. By introducing Prividium's blockchain-based architecture, market participants are able to gain access to automated, transparent, and continuous repo settlement, significantly reducing risk and unlocking new efficiencies across the transaction life cycle. While operational and regulatory considerations remain, the adoption of advanced digital infrastructure marks a promising step toward a more resilient and agile repo ecosystem.

For adoption at scale, institutions must address:

- **Regulatory alignment:** Clear frameworks for stablecoins, collateral treatment, and FMI licensing.
- **Governance models:** Shared standards for smooth on-chain collaborations.
  - **Integration:** Secure onboarding with existing core banking and custody systems.
  - **Risk controls:** Robust oracles, AML/KYC enforcement, and clear auditability.

"Institutions don't want to maintain a patchwork of bespoke bridges, what they need is a secure standard for interoperability. A unified interoperability infrastructure delivers that by providing a single solution that connects public and private blockchains while preserving privacy and enabling atomic settlement of complex workflows like delivery-vs-payment. By reducing the operational burden of cross-chain integration and embedding compliance and confidentiality at the infrastructure level, this gives institutions a standardized way to scale blockchain initiatives without adding risk."

Fernando Vazquez
President of Banking & Capital Markets
Chainlink Labs

Next steps

ZKsync Prividiums are no longer just a concept—they are already live. Prividiums are running on mainnet today, with more scheduled to be announced before year-end. This momentum underscores both the demand for the technology and its readiness for institutional-scale deployment.

To build on this progress, the Matter Labs team will continue expanding collaboration through structured demos and working groups. These forums bring together key stakeholders, subject matter experts, and infrastructure partners to tackle high-impact use cases such as cross-border payments and intraday repos, where Prividiums can deliver immediate value. By conducting real-value transactions between Prividiums, participants can define clear objectives and success metrics while aligning initiatives with strategic business needs.

In parallel, Matter Labs is engaging directly with institutions on a one-to-one basis to scope tailored deployments. Whether through collaborative working groups or private discussions, the goal is to help enterprises address their unique operational, regulatory, and integration requirements while contributing to the evolution of a shared settlement standard.

As adoption accelerates, insights from early deployments will inform a broader roadmap for industry-wide adoption, including best practices for deployment, governance frameworks, and common interoperability standards. By acting decisively and collaboratively, the financial services community can ensure it is at the forefront of this transformation—driving efficiency, transparency, and innovation through ZKsync Prividiums.

"From a wider industry perspective, the work being undertaken by SODA–the Standards Organization for Digital Assets–will ultimately create a standardized set of specifications for all the call functions in both these use cases, which can be applied to tokens on all blockchains. The project is being co-chaired by MIT and will start publishing the open specifications in 2026. Once operational, the standardized spec can be used by all blockchains and bridge providers for all tokenized transactions in regulated finance regardless of which blockchain is being used to issue the token."

Chris Ostrowski, SODA Services Ltd.

Conclusion

Financial markets demand faster, private, always-on settlement. Legacy systems cannot deliver it. Public blockchains cannot deliver it.

Prividiums can.

They are the first system to combine privacy, compliance, scalability, and interoperability into a single enterprise-ready EVM blockchain framework. By leveraging advanced ZK proof technology, Prividiums enable confidential, trust-minimized transactions that are both cost-efficient and compliant. Their hybrid architecture allows institutions to maintain full control over sensitive data while benefiting from the security and network effects of public Ethereum. The customizable nature of Prividiums ensures that organizations can tailor their environments to specific operational needs, whether for cross-border payments, intraday repo transactions, or other high-impact use cases.

With live Prividium applications and proven demos of private interoperability, as well as validation from this exercise, Prividiums stand as a credible path forward for institutional blockchain adoption.

By enabling secure, efficient, and private settlement across diverse networks, ZKsync Prividiums offer financial institutions a powerful tool to modernize their operations, reduce risk, and unlock new opportunities in the evolving global marketplace. As adoption accelerates, Prividiums are positioned to become the default infrastructure layer for financial markets—unlocking liquidity, reducing risk, and enabling institutions to thrive in the digital economy.

Appendix

Glossary

Anchoring: Submitting cryptographic proofs or hashes from a private or layer 2 blockchain to a public blockchain for security, auditability, and data integrity.

Appchain: A blockchain dedicated to a specific application or function, often used for specialized financial market infrastructure.

Atomic settlement: A process ensuring all parts of a transaction complete successfully together, or none do, preventing partial or failed settlements.

Audit trail: A record of all transactions and actions, enabling traceability and regulatory compliance.

Blockchain: A distributed, immutable digital ledger that records transactions in blocks linked together chronologically and cryptographically.

Burn and mint: A mechanism for transferring assets between blockchains. Destroy asset on source chain and create on destination chain.

Collateral: Assets pledged to secure a financial transaction, which may be forfeited if obligations are not met.

Compliance screening: Processes (often automated) to ensure transactions meet regulatory requirements, such as KYC, AML, and sanctions checks.

Consensus: The process by which blockchain networks agree on transaction validity and ledger state.

Consensus mechanism: The algorithm or protocol by which a blockchain network agrees on the validity of transactions (e.g., Proof of Authority, Proof of Stake).

Correspondent bank: A bank that provides services on behalf of another bank, often used in cross-border payments and settlement.

Cross-border payments: Transactions where the sender and recipient are in different countries, involving currency conversion and regulatory compliance.

Custodian: A financial institution or entity responsible for safeguarding assets, such as securities or digital tokens, on behalf of clients.

Data availability: Ensuring that transaction and state data are accessible to network participants, either on-chain, via third-party providers, or through private databases.

Daylight settlement risk: The risk that a transaction may not settle within the same business day, potentially leading to credit exposure or liquidity challenges.

EVM (Ethereum Virtual Machine) equivalence: Ability to run Ethereum-compatible smart contracts and applications without modification.

Ethereum: A public blockchain platform supporting smart contracts and decentralized applications, often used as a settlement layer.

Escrow smart contract: A smart contract that holds assets from multiple parties and releases them only when agreed conditions are met.

Finality: The point at which a transaction is considered irreversible and permanently recorded on the blockchain.

FMI (financial market infrastructure) chain: A dedicated blockchain or appchain coordinating liquidity, clearing, and settlement among institutions.

Gas token: The currency used to pay transaction fees on a blockchain network (e.g., Ether on Ethereum).

Gateway: Middleware that facilitates communication and proof aggregation between different blockchains or layer 2 environments.

Interoperability: The ability for different blockchains or systems to communicate, exchange assets, and share data securely.

Layer 1 (L1): The base blockchain protocol (e.g., Ethereum) responsible for core transaction processing and security.

Layer 2 (L2): A secondary protocol built atop L1 to increase scalability and speed and reduce costs by processing transactions off-chain.

Liquidity: The ability to quickly and easily convert assets to cash or other assets without significant price impact.

Lock and mint: A mechanism for transferring assets between blockchains. Lock asset on source chain and mint equivalent on destination chain.

Merkle proof: A cryptographic proof used to verify the inclusion of a transaction or data in a block, leveraging Merkle tree structures for efficiency.

Middleware: Software that connects different systems, enabling communication and data exchange between blockchains or applications.

Multi-node setup: A blockchain deployment with multiple independent nodes, enhancing resilience, decentralization, and operational continuity.

Native interoperability: Direct, protocol-level communication between blockchains or L2 networks, enabling secure and private asset transfers.

Omnibus account: A single account used to hold assets for multiple clients or institutions, simplifying settlement and reconciliation.

On-chain: Transactions or data recorded directly on the blockchain.

Off-chain: Transactions or data processed outside the blockchain, often for privacy or scalability.

Oracles: External data providers that supply real-world information (e.g., FX rates) to smart contracts on a blockchain.

Permissioned blockchain: A blockchain where participation and access are restricted to approved entities.

Prover: A system or module that generates ZK proofs to validate transaction correctness without revealing sensitive details.

Proving cost: The computational and financial cost associated with generating ZK proofs for transaction validation.

Role-based access control (RBAC): A system where access to data or functions is managed according to user roles, enhancing security and compliance.

Root hash: A single hash representing the entire set of transactions or data in a block, used for verification and anchoring.

Sequencer: A component in L2 blockchains responsible for ordering and batching transactions before they are processed and finalized.

Settlement cycle (T+1/T+2): The time between a transaction's execution and its final settlement, commonly one or two business days.

Smart contract: Self-executing code on a blockchain that automatically enforces terms and business logic when conditions are met.

Stablecoin: A cryptocurrency designed to maintain a stable value, typically pegged to fiat currency or other assets.

Tokenization: The process of representing real-world assets (e.g., securities, currency) as digital tokens on a blockchain.

Travel Rule: A regulatory requirement for financial institutions to share information about the originator and beneficiary of certain transactions, aimed at preventing money laundering.

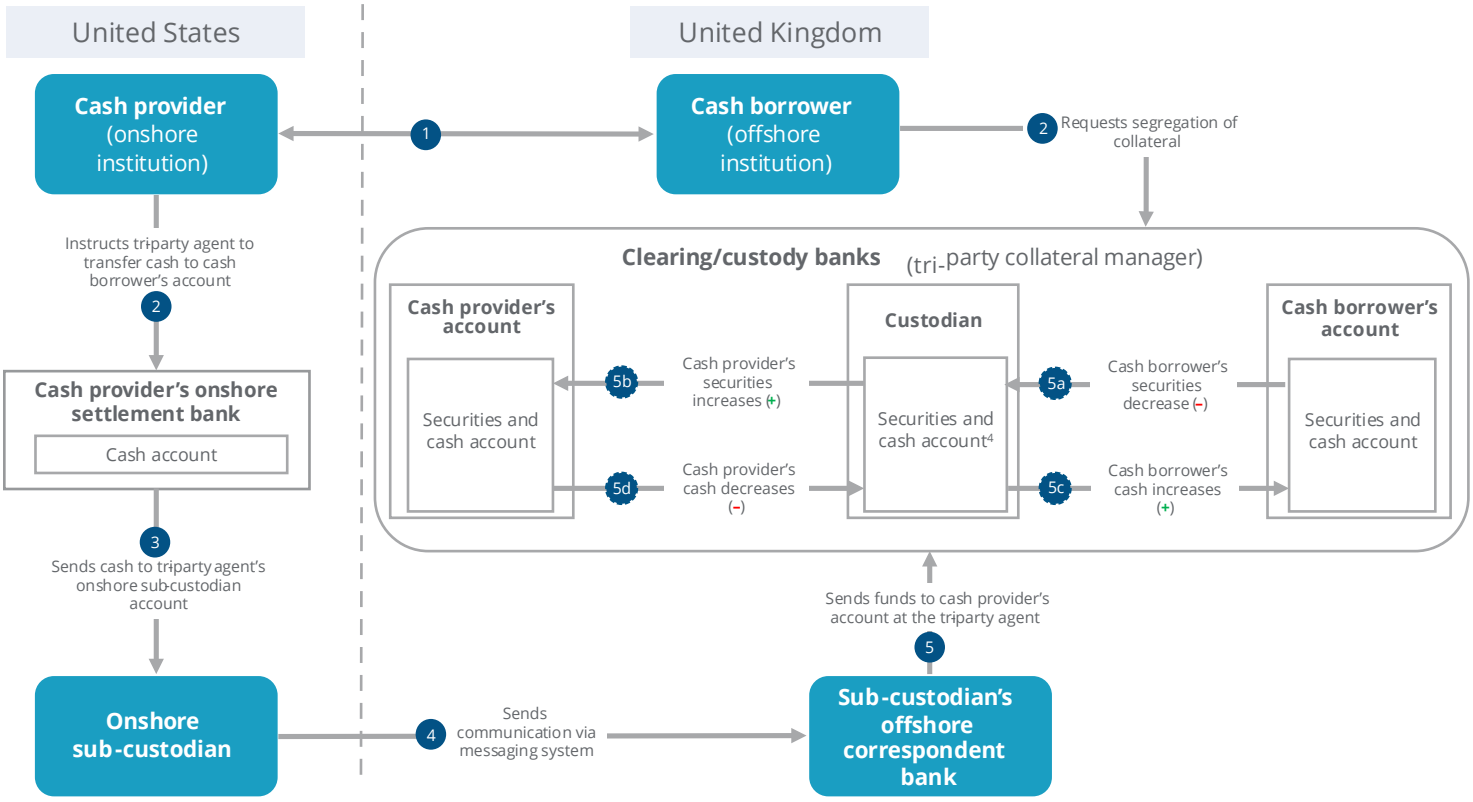
ZK proof: A cryptographic method allowing one party to prove a statement is true without revealing the underlying data.

zkEVM: A zero-knowledge Ethereum Virtual Machine, enabling private, scalable, and EVM-compatible smart contract execution.

Offshore tri-party intraday repo

An offshore tri-party USD repo is a repurchase agreement conducted in US dollars outside the United States, with the involvement of a third-party clearing agent. This arrangement is commonly used by international institutions that wish to utilize their US dollar-denominated assets for short-term funding needs. In this structure (figure 6), the third-party agent is responsible for managing the collateral and overseeing the transaction process, which enhances operational efficiency and reduces counterparty risk for both parties involved.

Figure 6. Offshore tri-party intraday repo



Current offshore tri-party intraday repo steps:

1. **Execution and confirmation:** The cash provider (onshore institution) in Country A (US) executes and confirms the trade with the cash borrower (offshore institution) in Country B (UK).
2. **Instruction to tri-party agent:** The cash provider instructs the tri-party agent to transfer cash to the cash borrower's account.
3. **Cash transfer:** The cash provider's onshore settlement bank sends cash to the tri-party agent's onshore sub-custodian account.
4. **Communication via messaging system:** The onshore sub-custodian sends communication to the sub-custodian's offshore correspondent bank using a messaging system.
5. **Funds transfer to cash provider:** The sub-custodian sends funds to the cash provider's account at the tri-party agent and requests segregation of collateral with the custodian bank (acting as the tri-party collateral manager).
   a. Cash provider's cash decreases.
   b. Cash provider's securities increase.
   c. Cash borrower's cash increases.
   d. Cash borrower's securities decrease.

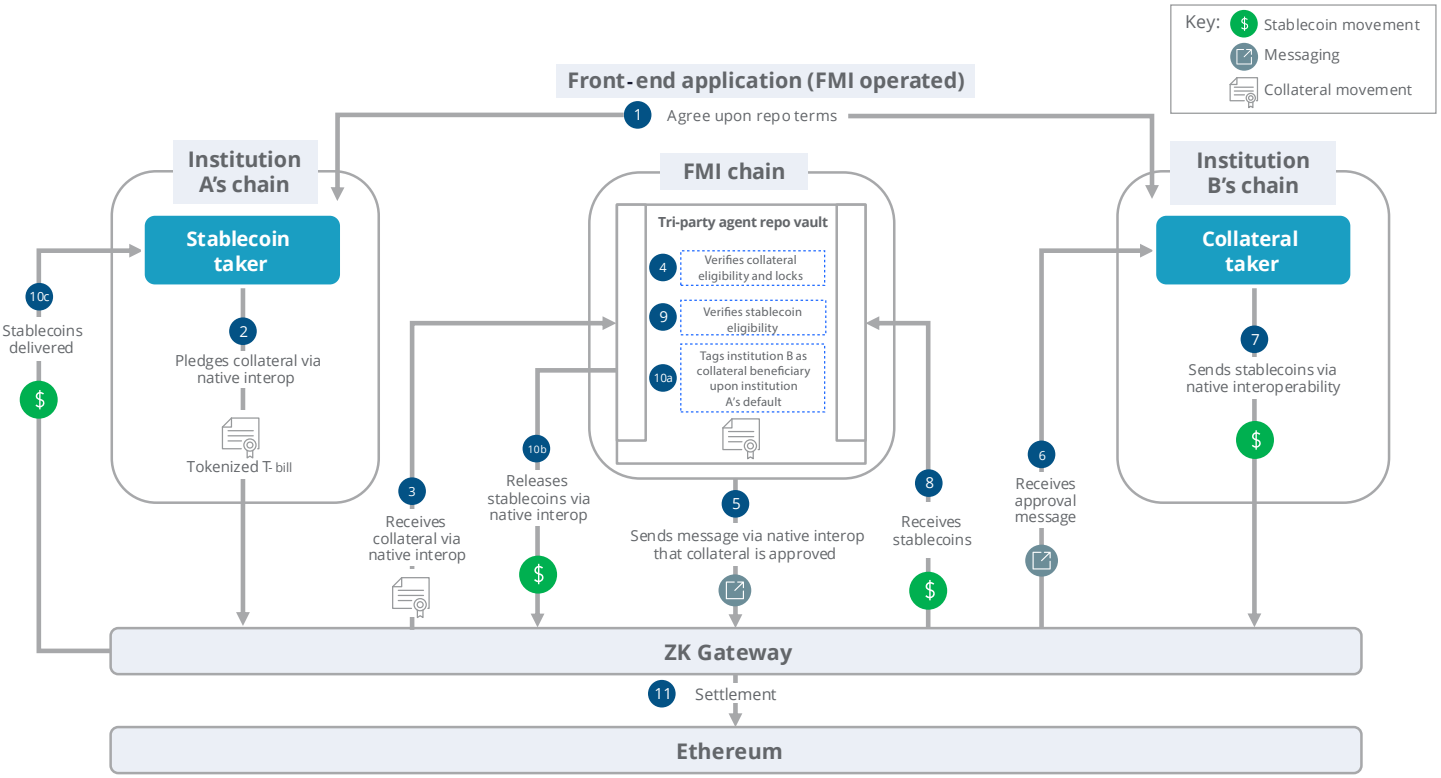
Current intraday repo workflows are routed through a labyrinth of intermediaries, including multiple layers of custodians and sub-custodians, correspondent banks, tri-party agents, and dollar settlement banks. Each transaction triggers a series of SWIFT MT messages, often multiple sets per participant, moving back and forth to facilitate instructions, confirmations, and reconciliations. This intricate web of messaging and account movements introduces numerous manual touchpoints and reconciliation cycles, each with its own potential for delays or mismatches. As cash and securities must pass through a chain of omnibus and segregated accounts before final settlement, operational, counterparty, and daylight credit risks are amplified at every stage.

Prividium tri-party intraday repo

The following assumptions were made for this process flow:

- An FMI chain is introduced to serve as a neutral, automated tri-party agent, providing the foundational platform for the marketplace system.
- The initial technology sessions will concentrate on the bilateral intraday repo use case; however, the underlying technology is readily adaptable to tri-party repo scenarios, which will be examined in subsequent phases.
- Institution A functions as the stablecoin taker. Institution B acts as the collateral taker.

Figure 7. Tri-party intraday repo flow



Tri-party intraday repo flow steps:

1. Institution A (stablecoin taker) and B (collateral taker) agree to the repo terms.
2. Institution A then pledges its collateral (e.g., a tokenized T-Bill) via native interop to the FMI chain.
3. FMI chain receives collateral via native interop.
4. The FMI chain programmatically verifies if the collateral is eligible for the transaction and locks it.
5. Collateral approve message is sent via native from the FMI chain.
6. Institution B (collateral taker) receives approval message.
7. Institution B pledges stablecoins via native interoperability.
8. FMI chain receives stablecoins.
9. FMI chain verifies the eligibility of the stablecoins.
10. a. Tags institution B as the collateral beneficiary upon institution A default.
    b. The FMI chain releases stablecoins via native interop.
    c. The stablecoins are delivered to institution A.
11. The entire flow is settled on Ethereum via ZK proofs.

Privacy solution to pain points

Current privacy solution pain points	Subtopics	Prividium solutions
Privacy and control	Confidentiality (addresses, balances, transfers)	Transactions execute off-chain; Ethereum receives only a ZK proof, so all raw data stays inside the chain operator's database.
	Fine-grained access controls	A private, gated RPC enforces role-based read/write permissions on every call.
	Compliance and auditability	Gated block explorer and local data storage let operators grant auditors/regulators full transaction access on request.
	Governance and trust assumptions	As an enterprise, you can run the sequencer and prover yourself, anchor proofs to Ethereum, and avoid any third-party control.
Performance	Throughput	Now: 200 TPS in production, 200ms block times, proof times <1s. Coming Q4 2025: 10,000 TPS.
	Cost	$0.0001/transaction proving costs on commodity graphics processing units (GPUs) (L4s) with Airbender.
	Finality	Finality on Ethereum from minutes (now) down to seconds (Q4 2025).
User and developer experience	UX (e.g., MPC and smart contract wallets, passkeys)	No customizations required to plug into existing wallet infrastructure or custodial solutions (e.g., Fireblocks, Blockdaemon).
	DevEx (e.g., EVM, leverage existing apps)	EVM equivalence. No smart contract refactoring; use tooling such as Foundry and Hardhat out of the box. Deploy any popular EVM app (e.g., AAVE, Uniswap, Morpho) or any EVM ZK privacy app (e.g., Paladin).
	Integration with existing systems (e.g., auth servers)	No custom token standards; use ERC-20s and other ERC token standards out of the box.
	Open-source	ZK proof technology is fully open-source. Upgraded ZK virtual machine (zkVM) and open-source proof system open sourced under Apache 2.0 and MIT licenses.
Trust minimized interoperability	Costs associated with transaction interactions	Interoperability significantly lowers costs by using ZK proofs to prevent fraudulent transactions, reducing legal expenses. With Prividium's interoperability, collateral can be atomically released between institutions upon rapid Ethereum settlement.

Current stablecoin clearing solutions

To address these risks, a variety of stablecoin clearing models have been deployed, leveraging the 24/7 availability of blockchain technology to enhance transaction efficiency and mitigate settlement challenges. Each emerging model presents a unique framework for managing counterparty exposure, liquidity, and transaction finality, while introducing distinct considerations around scalability, interoperability, and regulatory compliance. Table 1 provides a comparative overview of these clearing solutions.

Table 1. Current stablecoin clearing solutions

Clearing stablecoin	FMI liquidity appchain	Prefunded shared ledger model	Internal treasury swap/desk model	Tri-party custodial reserve model	Institutional stablecoin liquidity venue
Description					
Fully collateralized clearing stablecoins backed by multiple approved assets, which enables 24/7 minting and redemption capabilities through a smart contract subject to the collateral that backs the stablecoin.	Permissioned blockchain provided by a licensed FMI, where multicurrency pools of approved, tokenized assets exist on the FMI chain. The originator and beneficiary chains can use smart contracts for FX clearing and settlement, eliminating correspondent settlement flows experienced today.	Single permissioned ledger provided by one private institution or provider network with pre-funded multicurrency balances, allowing for near real-time balance updates on specific ledgers.	The bank or fintech converts incoming tokens using its own inventory, credits the customer, and holds the token—assuming price and capital risk until redemption or reuse.	Institutions maintain pre-funded cash accounts with a shared custodian. The clearing platform manages token transfers between these institutions by minting new tokens when cash is deposited and burning tokens when cash is withdrawn. Throughout this process, cash balances are updated (rebooked) by the custodian, ensuring that every token is fully backed by actual funds. This structure enables secure transfers without introducing counterparty risk.	The platform allows institutions to access stablecoin FX quotes from a number of different liquidity providers, where they can negotiate off-chain and settle on-chain via escrow smart contracts.

Clearing stablecoin	FMI liquidity appchain	Prefunded shared ledger model	Internal treasury swap/desk model	Tri-party custodial reserve model	Institutional stablecoin liquidity venue
Process					
i. Bank A would look to mint a clear USD stablecoin (a clearing stablecoin) by depositing its Bank A stablecoin into a smart contract. ii. That clear USD is redeemed by another bank or beneficiary bank from a reserve pool. iii. Bank B stablecoin is delivered to Bank B, allowing for settlement to take place in that preferred settlement asset without having exposure to the Bank A stablecoin.	i. Originating bank chain asks the FMI chain for an executable quote. ii. The FMI smart contract returns the quote, which is approved by both the originator and beneficiary. iii. To transfer the originating currency, USD as an example, the originator bank chain mints the USD stablecoin, then transfers it to the FMI appchain. iv. An FMI smart contract swaps the incoming USD for the beneficiary bank's stablecoin using pooled liquidity. v. The FMI appchain sends the beneficiary bank's stablecoin to the beneficiary bank chain, crediting the beneficiary's account.	i. Banks can wire fiat funds into an omnibus account that consists of a currency pair between, for example, USD and SGD. ii. The ledger issues equivalent or mints tokens onto the network. iii. A transfer is initiated by Bank A to instruct a debit of a specific number of US dollars to Bank B. iv. The ledger debits Bank A, credits Bank B, so finality is immediate. v. Bank B can swap USD to SGD as given by the pre-funded accounts.	i. FX desk quotes an amount of a specific currency, once again SGD, for an amount of USDC payment. ii. Client of FX desk accepts the rate and sends 10M USDC to the bank's treasury wallet. iii. There is a stablecoin receipt where the USDC lands in the bank's treasury wallet and is timestamped and reconciled to the payment instruction. Based on the pre-agreed FX rate, the bank can immediately credit the corresponding SGD amount needed to the client's domestic account through the internal ledger, and no on-chain swap is needed. iv. The bank's treasury desk now holds the USDC as inventory and books the FX spread, so it can redeem the USDC for fiat later.	i. Sender institution submits a payment using a preferred stablecoin. ii. The platform determines that the receiver prefers a different token. iii. Custodial rebooking occurs; the platform instructs the shared custodian to move cash between issuer sub-accounts. \iv. The sender's token is burned, and the receiver token is minted and delivered, which is the token conversion step. v. The receiver institution delivers the preferred token to the client. Note: The fiat is moving at a sub-account level at the custodian bank, and the actual stablecoins are minted and burned between two institutions across any type of blockchain.	i. User requests a firm quote to convert one stablecoin into another. ii. Negotiation occurs where a number of liquidity providers review and respond to that quote. iii. A quote is found that works for both sides. iv. Trade match occurs, in which best quote is selected, and terms are agreed upon with chosen market maker. v. Escrow funding occurs, in which both parties deposit both side's stablecoins into a smart contract to achieve atomic settlement. vi. Settlement and confirmation occur, in which the contract is executed, stablecoins are swapped, and delivery is confirmed to both parties.

Clearing stablecoin	FMI liquidity appchain	Prefunded shared ledger model	Internal treasury swap/desk model	Tri-party custodial reserve model	Institutional stablecoin liquidity venue
Advantage					
i. Stablecoin conversion: Allows sender and receiver to settle in different stablecoins. ii. No pre-funding required: Today, stablecoin clearing requires multiple pre-funding steps throughout a transaction across different nostro/vostro accounts. iii. Diversified backing: Backed by a pool of stablecoins. iv. Minimal changes required for integration.	i. Limited pre-funding: Senders and receivers are not required to pre-fund their accounts, offering greater flexibility by eliminating the need to lock up capital in advance. This allows participants to optimize liquidity and deploy their funds more efficiently. ii. Single-hop FX and payment: One on-chain step with originator and beneficiary having the necessary relationship with the FMI chain, but doesn't require a web of correspondent bank relationships. iii. On-chain audit trail: Immutable logged by a licensed FMI, so any institution involved can look at the transaction history between different counterparties. iv. Consolidated liquidity: Having a few pools of liquidity replaces all nostro/vostro accounts, improving treasury capabilities.	i. Single Integration per participant: One API, no bilateral links. ii. No slippage: Since these are pre-funded balances, liquidity or slippage risks are reduced. iii. Straightforward multicurrency view: Since this all exists on one ledger with pre-funded accounts, there is the ability to see all of your positions within one dashboard. iv. Self-netting: Intraday self-netting reduces the number of settlements taking place on the individual network.	i. Immediate local-currency credit: Instant fiat credit, no external clearing. ii. Bank/fintech-controlled FX spread: FX rate set and margin captured. iii. Inventory optionality: Based off what is being custodied or owned by the FX desk; allows for greater optionality for stablecoin redemption or reuse. iv. Seamless client experience: No wallets or on-chain steps; this whole process happens within the books of the treasury desk.	i. No pre-funding required: Only issuers hold reserves at custodian banks. ii. Single-hop UX: No need for multiple correspondent banking networks to complete this transaction end to end. iii. Fiat-first finality: Cash is rebooked before the burning of token, so no de-peg risk introduced. iv. Fewer accounts: Given that there is only one or few custodians involved within the transaction flow, this reduces the amount of funding needed for multiple accounts.	i. Transparent price discovery: Institutions could go to several different venues to find the best pricing, reducing intermediation costs. ii. No central clearing party required. iii. No pre-funding required.

Clearing stablecoin	FMI liquidity appchain	Prefunded shared ledger model	Internal treasury swap/desk model	Tri-party custodial reserve model	Institutional stablecoin liquidity venue
Disadvantage					
i. Asset eligibility: If there are a number of different stablecoins with different regulatory frameworks, you may not be able to back a clear USD stablecoin with a foreign stablecoin without causing the clear USD stablecoin to not be payment stablecoin compliant under the GENIUS Act. ii. Reserve dilution: With multiple stablecoins with different reserve requirements, this could reduce redemption efficiency. iii. Cross-chain complexity: Managing transactions across multiple blockchain networks introduces several friction points for specific use cases. These include challenges with interoperability standards, increased risk of failed or delayed settlements due to differing consensus mechanisms, and the need for robust bridging protocols to ensure secure and reliable value transfer.	i. Liquidity provisioning: There still exists a need to seed the FMI pool. ii. Onboarding friction: Every bank and every multicurrency asset pool per jurisdiction must be whitelisted, given that it is a permissioned blockchain provided by a licensed FMI.	i. Omnibus-bank credit risk: Reliant on one institution acting as the network provider. If funds are frozen, or if the safeguarding bank fails, there exists significant capital lockup. ii. Single operator trust: If the operator is down or any malicious activity is taking place, it can stop all activities between other intermediaries. iii. Scaling: Each new currency needs its own new account, which requires pre-funding, legal setup, and capital.	i. Stablecoin balance-sheet exposure: De-peg, liquidity, and capital risk are heightened until the stablecoins can be sold back into the market to get the fiat. ii. Capacity limits: Transaction size limited by inventories and risk limits. iii. Single-desk dependency: Reliance on one unit for pricing, custody, and settlement. iv. No shared liquidity benefits: Liquidity siloed; no pooling or netting.	i. Liquidity lockup: Issuers need to pre-fund cash reserves at those specific custodians that are part of the transaction flow, which could strain balance-sheet capacity. ii. Custodian single-point risk: If there is one or multiple custodians, there could exist some reliance if there is an outage, which could halt all transaction activity. iii. Limited access reach: Only tokens whose issuers bank within the custodian are eligible.	i. Variable liquidity: Depth varies in larger trades with increased spreads during non-peak hours. ii. Quotes expire quick. iii. Information leakage: RFQ requests could reveal trade size and direction to multiple market makers, inviting wider spreads.

Current industry privacy solutions

Privacy solution design	Description
Public programmable privacy chains	• Uses non-EVM bespoke languages, making it difficult for users and developers since standard tools and protocols such as OpenZeppelin, Hardhat, Uniswap, and Aave aren't supported. • Slower proving times lead to higher costs, lower performance, and limited institutional integration or customization.
Privacy middleware solutions	• Can cause liquidity fragmentation, and observers can still see the deposits and withdrawals from the pool. • Other solutions do not hide addresses for token extensions and leave additional details such as metadata of the fact of a transaction and its occurrences available impacting overall privacy.
Special-purpose appchains	• Provide customizability through adding token extensions, tailoring validator sets, and selecting specific gas tokens. • Struggle with trust-minimized interoperability as they rely on trusted relayers.
Private payment networks	• Solely built for payments and do not have programmability to add features like automated market makers (AMMs) or swap solutions. • Interoperability and transaction per second limited to max ~25 TPS.
Enterprise DLTs/ consortium network	• Strong for access control and auditability as built for regulated participants. • Nuanced privacy as there is overhead required to set privacy groups for transactions between organizations without exposing it to other validators. • Does not enable trust-minimized interoperability; must rely on a mediator, synchronizer, or a legal agreement; and risks can open up to front-running or manipulated transactions.

Quantum resistance

ZKsync inherits quantum resistance through its ZK-STARK architecture. ZK-STARK-based proofs derive their security properties directly from the underlying hash function, primarily Blake2 in our implementation, and cryptographic hash functions are widely recognized as quantum-resistant primitives. User signatures are currently based on Elliptic Curve Digital Signature Algorithms that are not quantum resistant. ZKsync will need to upgrade to one of the many well-known quantum-resistant signature schemes such as NIST's FIPS 204, Module-Lattice-Based Digital Signature Algorithm.

Endnotes

1. Stripe, "How long do international payments take? What to know about international wire transfers", June 7, 2024
2. Keyrock and Bitso Business, *Stablecoin payments: The trillion dollar opportunity*, accessed September 2025, p.14.
3. CellPoint Digital, "The ultimate guide to cross border transactions," accessed September 2025.
4. NICE Actimize, "Mitigate AML risk in correspondent banking without resorting to de-risking," 2022.
5. Ibid.
6. Alberto Di Iorio, Anneke Kosse, and Ilaria Mattei, *Embracing diversity, advancing together—results of the 2023 BIS survey on central bank digital currencies and crypto*, BIS Paper No. 147, June 14, 2024.
7. Hoover Institute, "2024 Institutional Investor survey finds governance issues and climate concerns sway decision makers," April 30, 2024.
8. Wyden, "Solving liquidity fragmentation with a unified execution layer for digital assets," July 24, 2025.
9. Nefture Security, *The 2024 crypto crime report*, Coinmonks, June 13, 2025.
10. Financial Action Task Force (FATF), *Targeted updated on implementation of the FATF Standards on Virtual Assets/VASPs* (Paris, France) June 2024.
11. Gatenox, "2023's biggest AML fines: Who got caught, and why?," accessed September 2025.
12. Gautami Tripathi, Mohd Abdul Ahad, and Gabriella Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," Decision Analytics Journal 9 (December 2023); 100344.
13. Josh O'Sullivan, "Tokenize asset market to hit $10T by 203: Chainlink report," Cointelegraph, September 25, 2024.
14. Dun & Bradstreet, "Financial services: Research shows regulatory burden increased 35% YoY," August 29, 2024.
15. Broadridge, "Return on innovation: Intraday repo has arrived on scale," 2023.
16. Amrit Mohanty, "The real cost of settlement delays (and how to fix it with automation)," Optimus Fintech, May 6, 2025.
17. AQXT, "Unveiling the advantages of post-trade automation," August 8, 2024.
18. Basel Committee on Banking Supervision (BCBS), "Global systemically important banks—revised assessment framework," Bank for International Settlements (BIS), March 7, 2024.
19. BCBS, "Regulatory Consistency Assessment Programme (RCAP): Assessment of Basel NSFR regulations—Mexico," BIS, December 2023.
20. Coin Law, "KYC Compliance in Crypto Statistics 2025: Data Insights and Compliance Trends," June 16, 2025