PRIVIDIUM®

Proof-Based Private Interoperability: Extending Besu to Public Ethereum

ALEX GLUCHOWSKI, CEO | MATTER LABS | LF Decentralized Trust

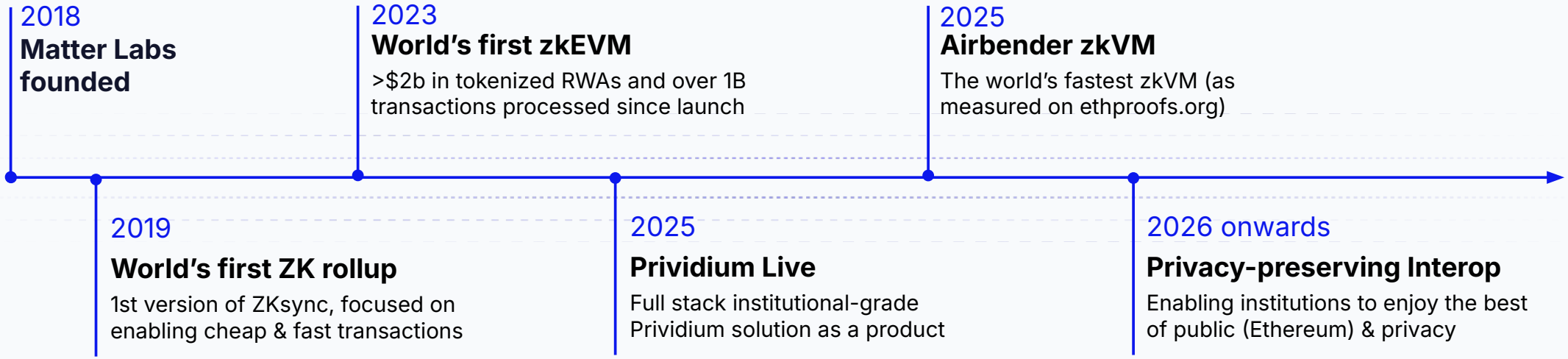
Matter Labs is the team that made ZK reality on Ethereum

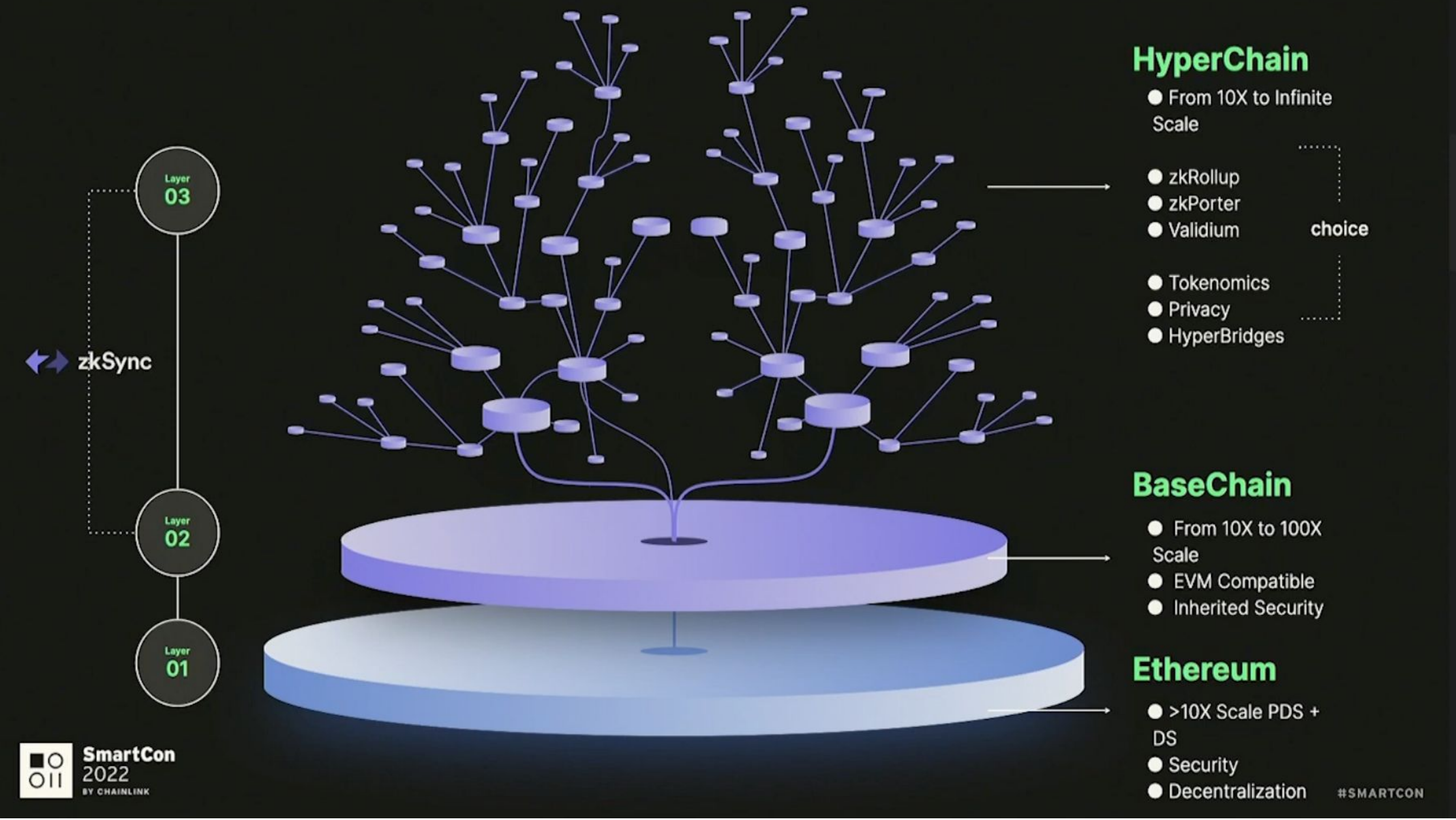
$258M
Raised from a16z et al.

6 Years
In Production

$4 Billion
Total Value Secured

>1 Billion
Transactions Processed




Layer 03
Layer 02
Layer 01
zkSync
HyperChain
From 10X to Infinite Scale
zkRollup
zkPorter
Validium
choice
Tokenomics
Privacy
HyperBridges
BaseChain
From 10X to 100X Scale
EVM Compatible
Inherited Security
Ethereum
>10X Scale PDS + DS
Security
Decentralization
SmartCon 2022
BY CHAINLINK
#SMARTCON

USE CASE

Cari: $600B private inter-bank tokenized deposit network







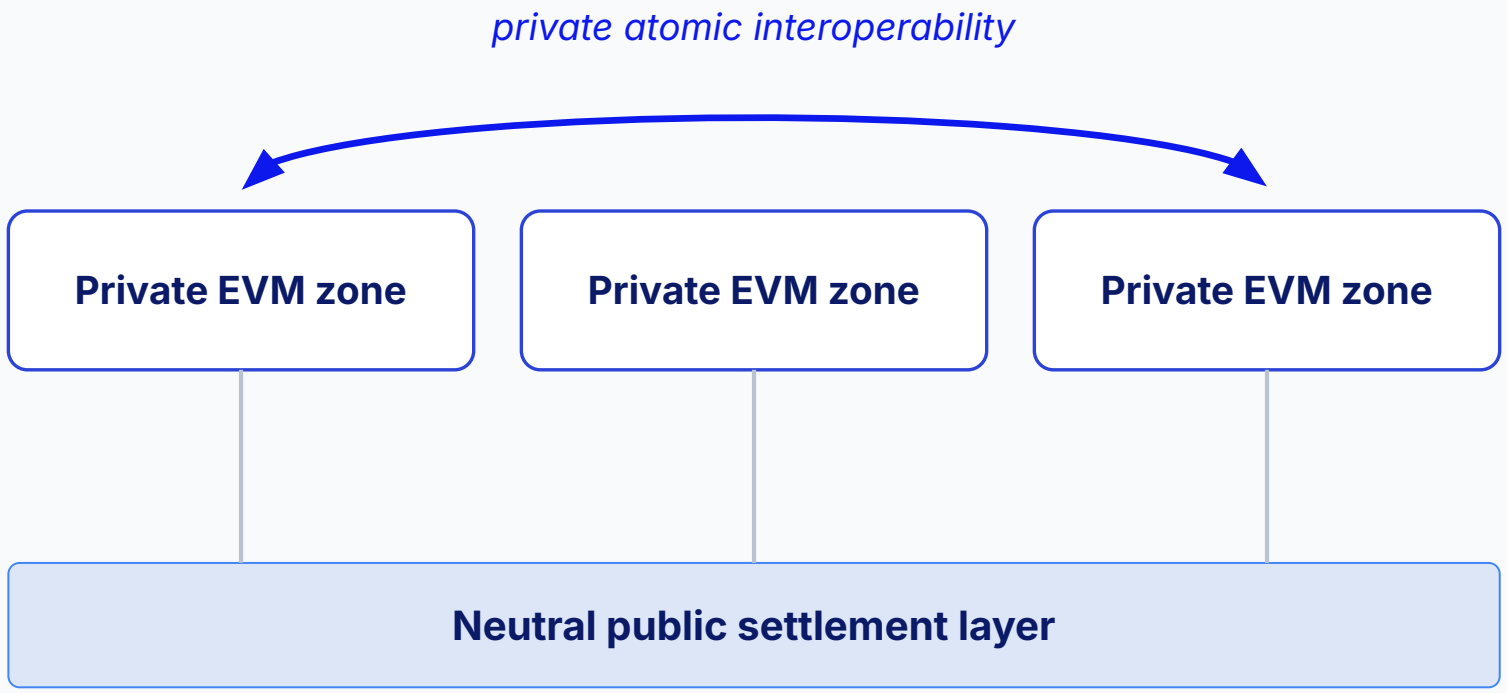




SOLUTION

Prividium: architecture overview

Each institution keeps full control of its own zone, and interoperates directly with every other.



TECHNOLOGICAL BREAKTHROUGH

Secured by ZK proofs, not trust in operator

Rules written as code, provable to authorized counterparties, auditors, and regulators under defined rules.

Programmable as EVM

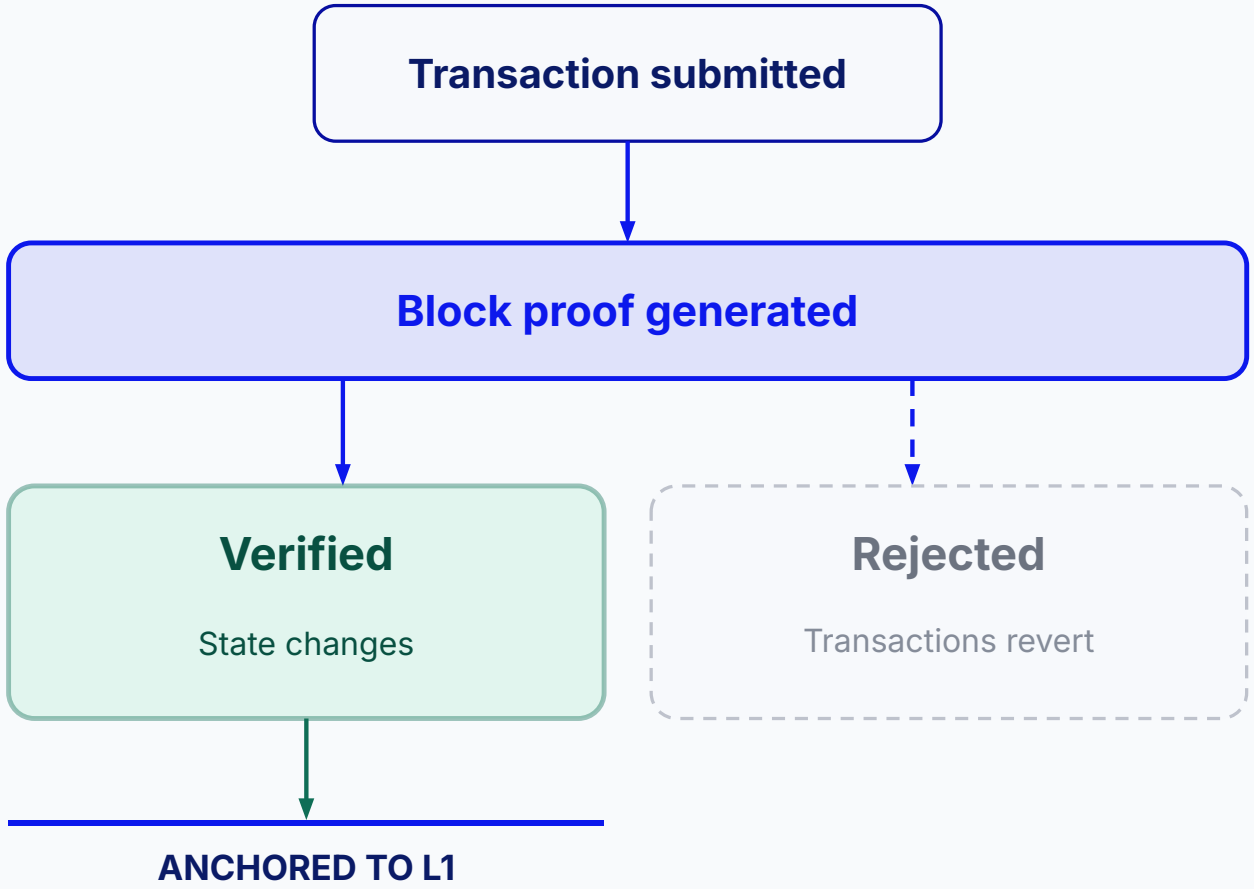
Limits, conditions, multi-party arrangements, compliance workflows, expressible as code in EVM.

Provable on demand

Counterparties and auditors verify any state, transaction, or event directly, without having to trust an operator.

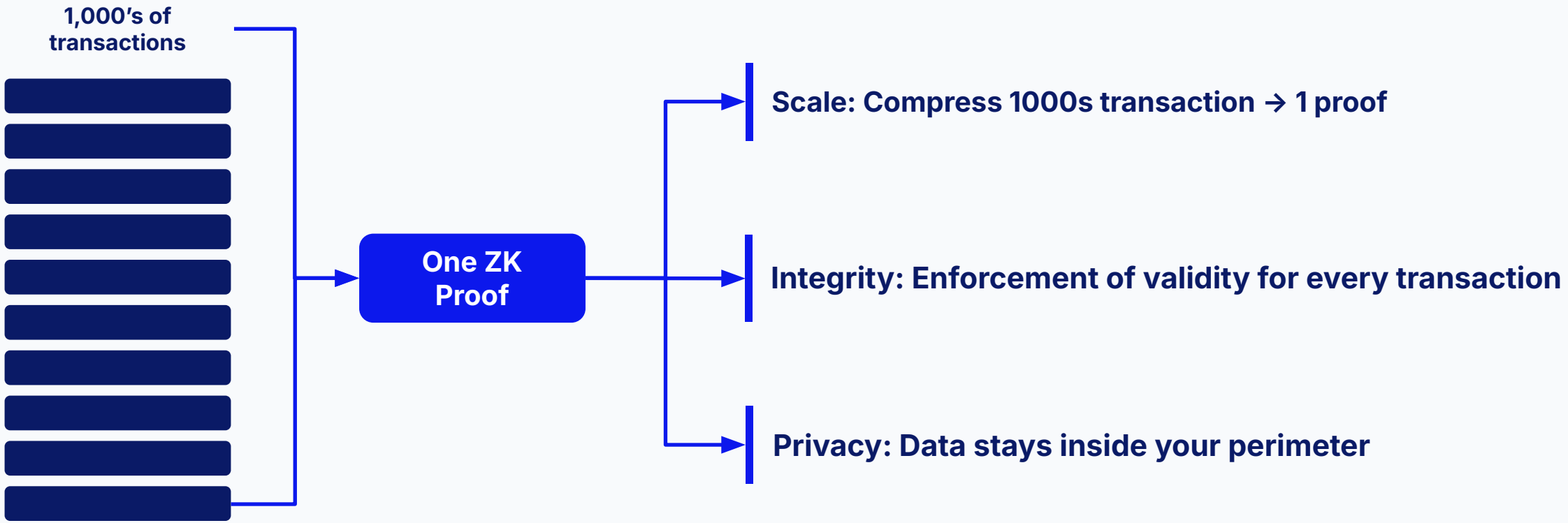
Defence in depth

Prividium runs inside the institution's security perimeter, providing extra layers of enforcement on top of the existing regime.



BREAKTHROUGH

ZK proofs deliver integrity and privacy at scale.



PROVER

EthProofs.org benchmark: Airbender, #1 zkVM for EVM

single-GPU

provers

multi-GPU single-GPU

prover	open source	binary available	avg time	avg cost
vast5090 ZKsync Airbender by MatterLabs	✓ prover	✓ reproducible	23.0s	$0.0034
zilkworm-hypercube SP1 Hypercube by Zilkworm	✗ prover	✓ reproducible	46.1s	$0.0069
SP1 Hypercube SP1 Hypercube by Succinct	✓ prover	✓ reproducible	1m 49s	$0.0211
Ethrex ZisK Prover (1x5090) ZisK by LambdaClass	✓ prover	✓ reproducible	1m 55s	$0.0285
ZisK ZisK by ZisK	✓ prover	✓ reproducible	2m 51s	$0.0329
powdr-OpenVM OpenVM by powdr	✓ prover	✓ reproducible	3m 5s	$0.0355
OpenVM OpenVM by Axiom	✓ prover	✓ reproducible	4m 14s	$0.0489
Ceno-1x4090	✗ prover	✓ reproducible	4m 22s	$0.0124

multi-GPU

provers

multi-GPU single-GPU

prover	open source	binary available	avg time	avg cost
Airbender 8x5090 ZKsync Airbender by MatterLabs	✓ prover	✓ reproducible	6.8s	$0.0071
ZkCloud Eth Prover v4 ZisK by ZkCloud	✓ prover	✓ reproducible	7.5s	$0.0450
ZisK Sevilla Cloud Cluster ZisK by ZisK	✓ prover	✓ reproducible	8.0s	$0.0249
Pico Prism Pico by Brevis	✓ prover	✓ reproducible	8.2s	$0.0685
ZisK Girona On-Prem Cluster ZisK by ZisK	✓ prover	✓ reproducible	8.4s	$0.0202

ZKsync

PERFORMANCE

Horizontally scalable throughput without loss of verifiability

Airbender zkVM converts execution traces of every tx into compact cryptographic proofs that Ethereum can verify.

< 1 sec

ZK finality at the protocol level

< $0.0001

Proving cost per transaction

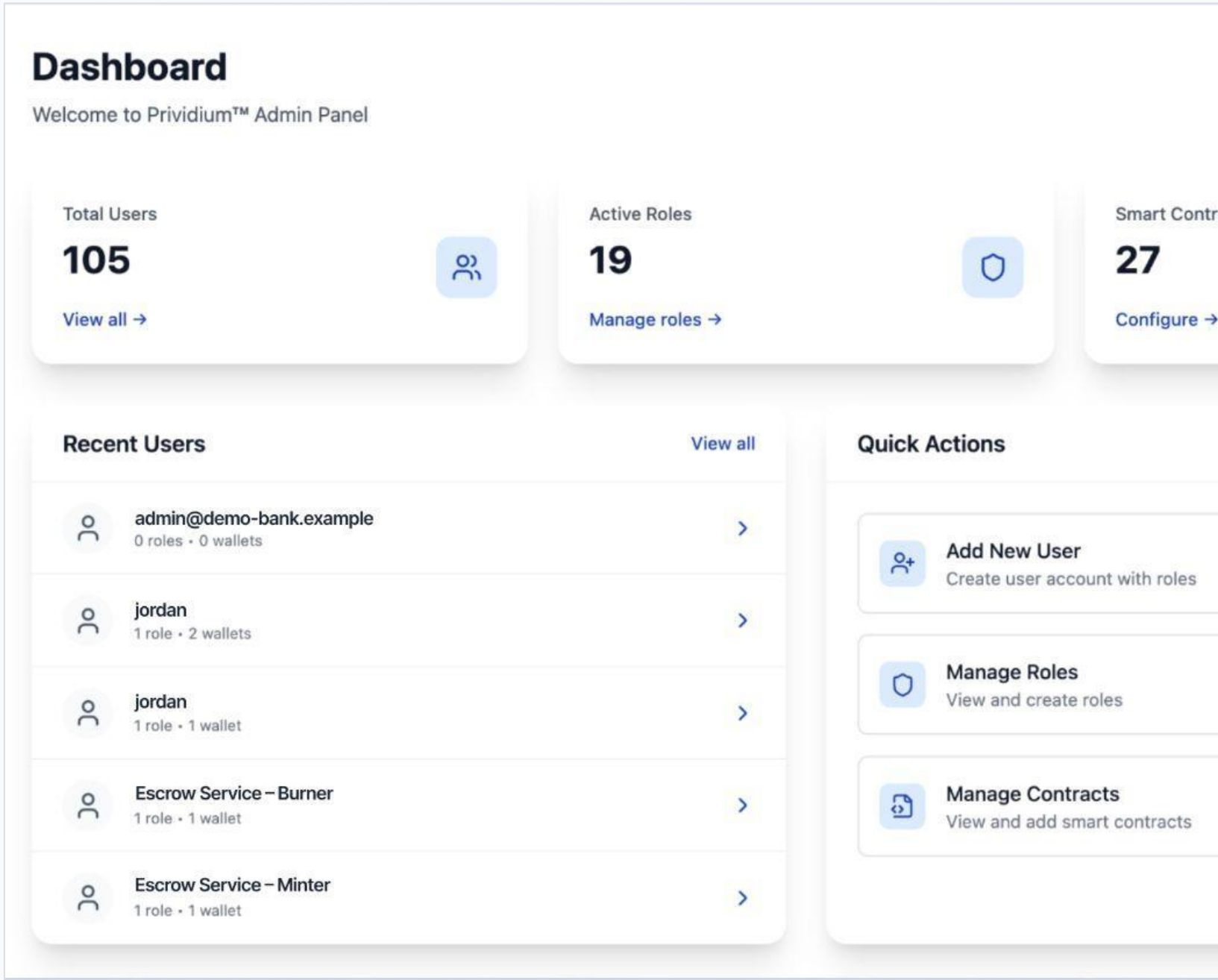
100,000+

TPS per Prividium

CONTROL

Full institutional Role-Based Control

- Each institution operates its own private zone with full ownership
- Granular access provisioning for user and role types
- Intuitive smart contract management with template permission controls
- Selective data disclosure to counterparties, auditors, etc



PRIVACY

Your data never leaves your perimeter

Privacy is a property of where data lives, not a policy you configure.

1 Created and held in your zone

Transactions execute and state is stored inside your own zone. Nothing is written to a shared environment you would later have to restrict.

2 Only proofs cross the boundary

What reaches Ethereum is a ZK proof, not the transaction. Amounts, terms, and counterparties stay inside your perimeter.

3 No third party ever holds your data

No operator, mediator, or counterparty sees it. There is no shared pool to misconfigure. The boundary is enforced by mathematics, not configuration.



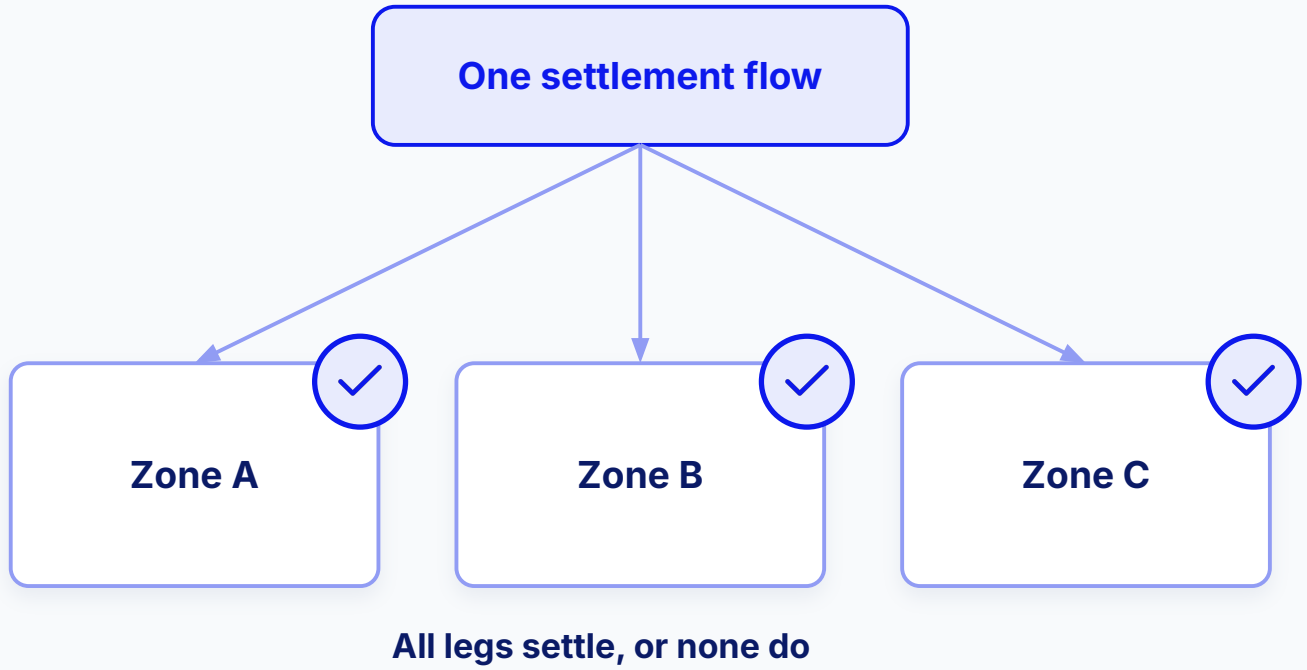
Only a proof crosses the boundary. The data stays inside.

Private atomic interoperability at scale.

A single transfer settles across multiple parties, at once

Privacy preserved for each party with finality anchored on Ethereum

Ideal for multi-counterparty operations and use cases



INDEPENDENT RESEARCH (UNDER EMBARGO)

SODA report: technical excellence → business value

44%

Stall in pre-production or scaling

The hardest phase for a private-chain pilot to clear, and the single biggest drop-off point

30%

Cite legacy-system integration

The largest named infrastructure gap: connecting the tokenized layer into existing bank systems

90%

Say external infrastructure is 1 to 3 years from maturity

Only 10% expect it within 12 months; no one calls it ready today

INTEGRATION

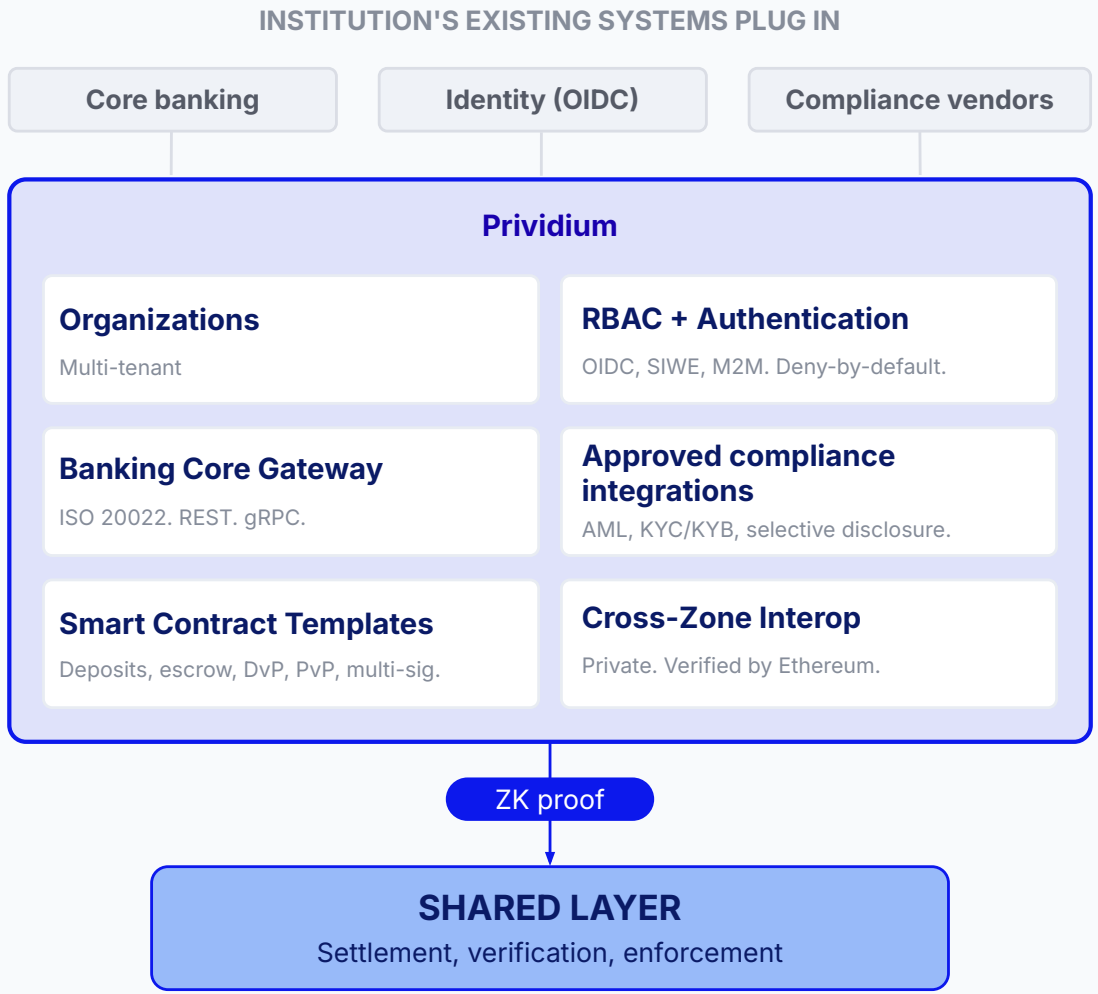
Modular design to plug into existing infrastructure.

Open, with no lock-in

Open what proves correctness and prevents lock-in; certified, supported service for production.

Plugs into existing systems

Adapters for core banking, custody, and payments, OIDC. Operational tooling included out of the box.



USE CASE

Multi-tenancy support

Institutional control extends from zone perimeter to individual wallets. Each layer independently auditable.



1 Zone-Wide Enforcement

The operator has full audit-level access over that zone. Zone A has no visibility into Zone B.

2 Organization Scope

No org can view another's data. Multiple orgs can share state via smart contracts.

3 User-Level Access

Users are bound to org and role. Different roles represent divisions, desks, or subsidiaries.

4 Wallet Provisioning

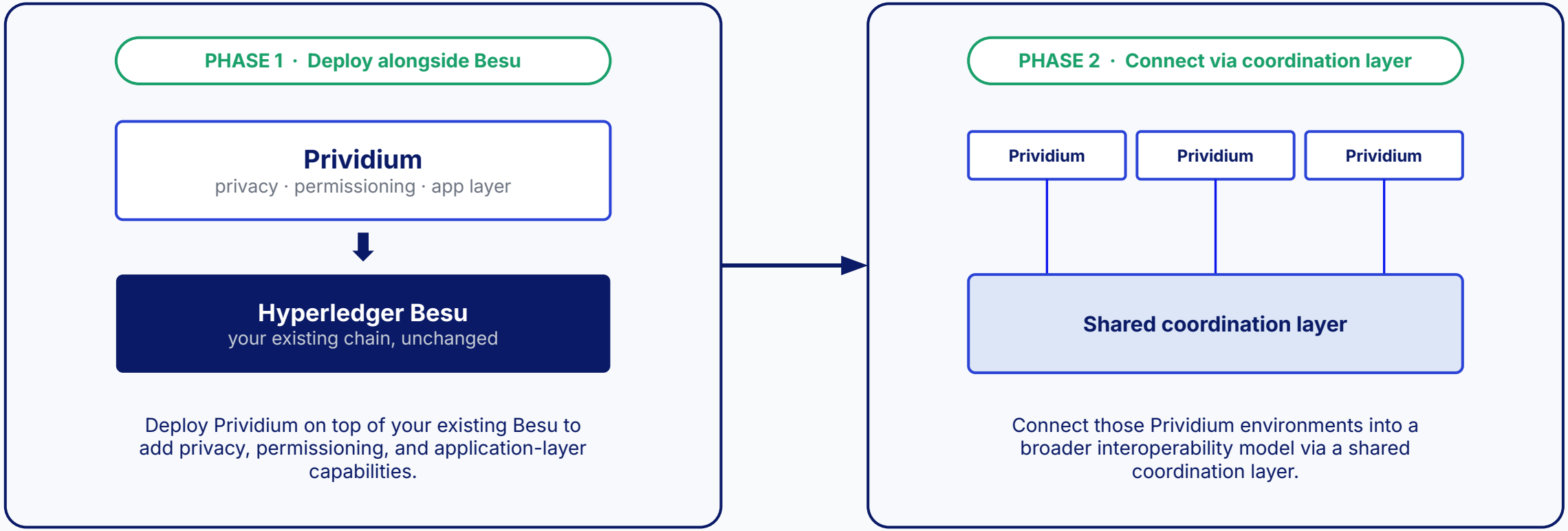
Each wallet is tied to a specific organization and user.

Prividium + Besu Support

Connecting to your existing infrastructure, with no migration required

A PATH AT YOUR SPEED

A phased path from Besu to full interoperability



No rip-and-replace. Besu carries through every phase; you adopt Prividium and connect to the network on your own timeline.

BUSINESS ADVISORY

From Strategy to Production



Use Case Scoping



Solution Architecture



Forward-deployed Engineering



Business Value Engineering

THANK YOU

Build on Prividium.
Anchor to Ethereum or Besu.

ALEX GLUCHOWSKI, CEO | ag@matterlabs.dev