Building a One-Way Mirror

Vendor-neutral privacy for **regulated finance**.

Igor Mandrigin · Co-Founder & CTPO, gateway.fm



0:00 +0:00



Gateway is the orchestration layer for production digital assets.

01 **Abstract complexity**
Infrastructure, privacy, identity, compliance, operations.

02 **Advisory and integration**
Design the path, connect the systems, get it live.

03 **First + third party services**
Gateway platform, partners, applications, and infra together.

0:00 +0:00

Which onchain use cases need privacy?

SELECTIVE DISCLOSURE — ACCESS CONTROL IS THE WHOLE JOB

Stablecoins | Payments | RWA tokenization | Bonds & debt | Money-market funds | Repo | Treasuries | Procurement | Registries | Supply chain

PAIR WITH CRYPTOGRAPHY — ACCESS LAYER PLUS ZK / FHE / TEE

Derivatives | FX | Commodities | Stocks | Identity | Oracles | Private reads | Messaging

OPERATOR MUST BE BLIND — NOT THIS PATTERN

Humanitarian disbursement | Civic participation | Identity continuity

Most regulated-finance use cases live in the first row — where selective disclosure is the whole job. **Almost all of them require privacy of some kind** — so we went looking for a solution, and ended up building our own. Source: EF IPTF 23-use-case catalogue.

0:00 +0:00

Pilot vs Production

01 **PoC**
happy path

02 **Ops**
keys, upgrades, observability

03 **Evidence**
the same audit trail under load



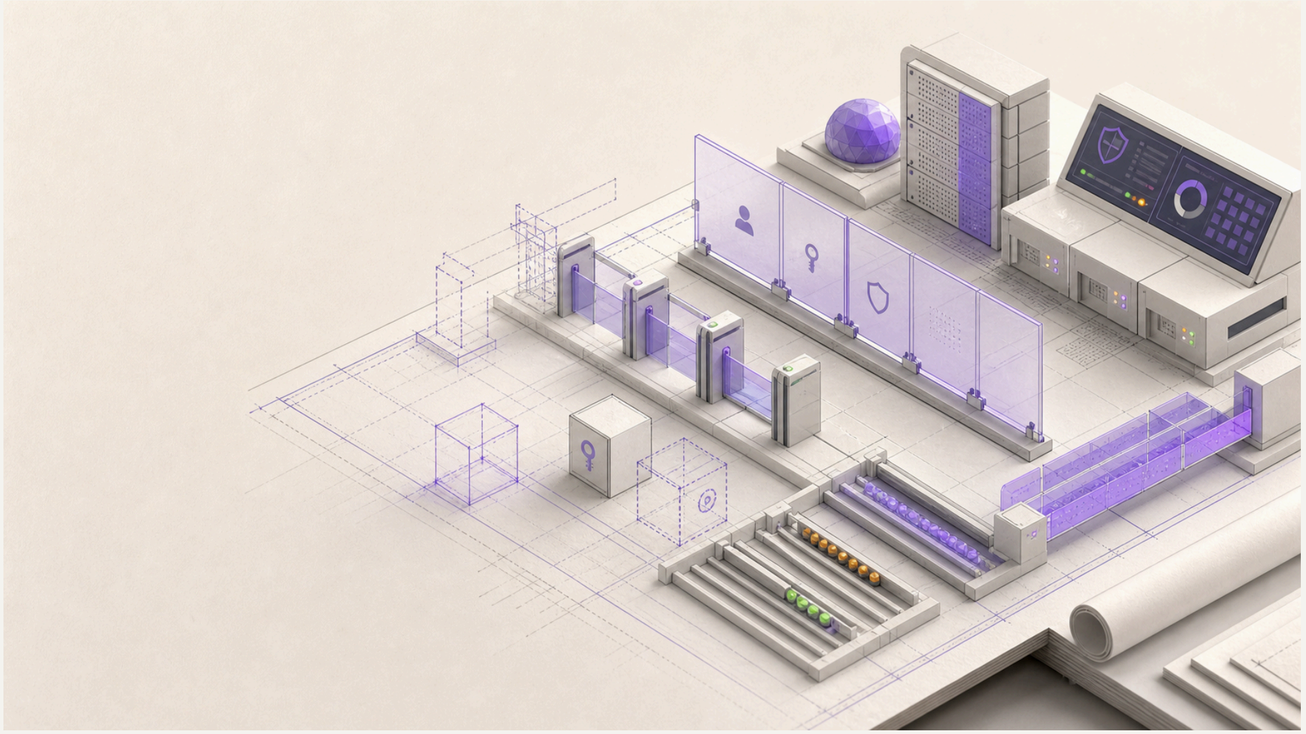
Designing for Production

01 **Engineering**
crypto, compatibility, integration surface

02 **Ops**
keys, upgrades, recovery, observability

03 **Risk**
operator trust, leaks, failure modes

04 **Governance**
roles, approvals, evidence, disclosure



0:00 +0:00

Decentralization theater

RARE

True decentralization

Open participation, independent operators, censorship resistance, governance that can actually say no.

COST

Very expensive

More parties, slower changes, harder incident response, more coordination, more duplicated infrastructure.

HONEST

Name the operated parts

Sequencers, RPCs, admins, provers, policy services, bridges, and support are usually operated systems.

0:00 +0:00

Institutional knowledge

IAM

Microsoft Entra ID, JWTs, did:iden3, roles, approvals, change control.

DEV

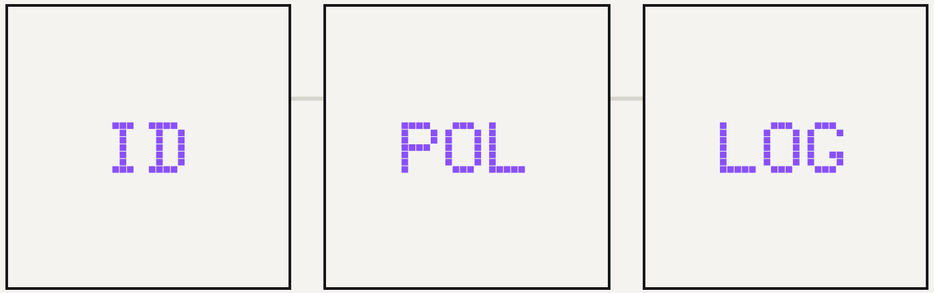
EVM compatibility, JSON-RPC, events, indexers, Foundry, Hardhat, cast, wallets.

OPS

IaC install trails, audit evidence, reviewed policy changes, runbooks, support model.

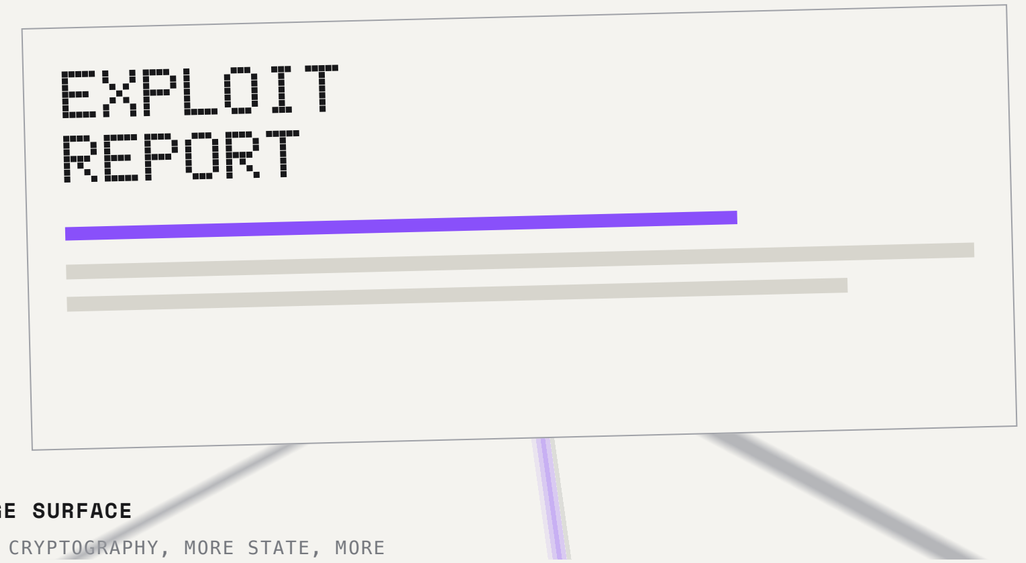
0:00 +0:00

Simplicity



SMALL SURFACE

IDENTITY, POLICY, EVIDENCE.
FEWER MOVING PARTS TO REASON
ABOUT.

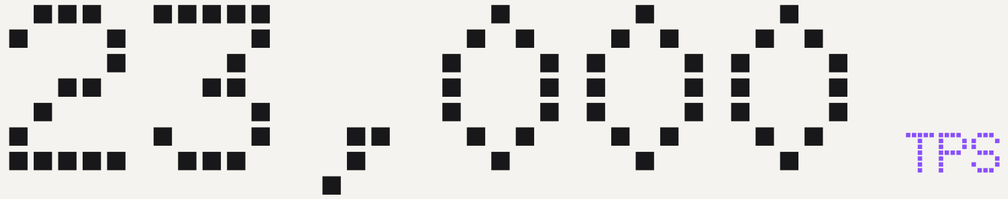


LARGE SURFACE

MORE CRYPTOGRAPHY, MORE STATE, MORE
CEREMONIES, MORE PLACES TO MISS ONE
ASSUMPTION.

Privacy cannot be the bottleneck.

TESTED ON AWS HARDWARE

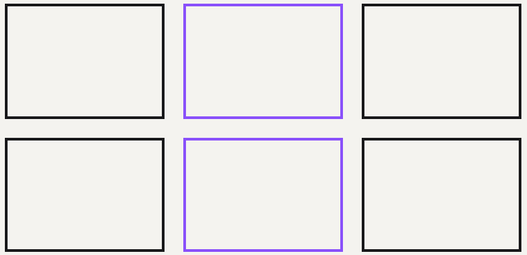


RETH EXECUTION

<1S CONFIRMATION TARGET

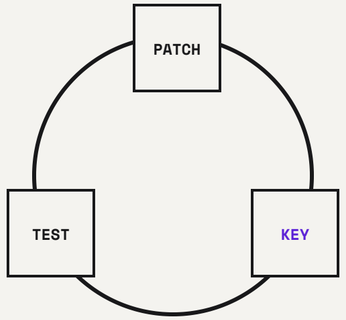
PRIVACY AT THE EDGE

Cost



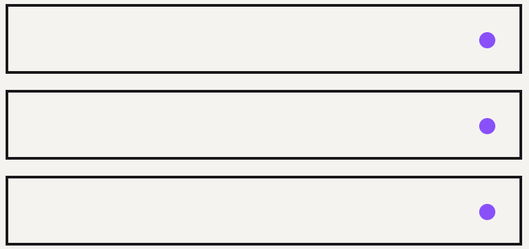
Setup

ARCHITECTURE, INTEGRATION,
CEREMONIES, FIRST AUDIT.



Maintain

UPGRADES, ROTATIONS, REVIEWS,
INCIDENT DRILLS.



Hardware

PROVERS, COPROCESSORS,
ENCLAVES, RPC EDGE CAPACITY.

Selective Disclosure



External assurance

Auditors, regulators, counterparties, insurers.



Control evidence

Show access, change, disclosure, and exception records.



Retention period

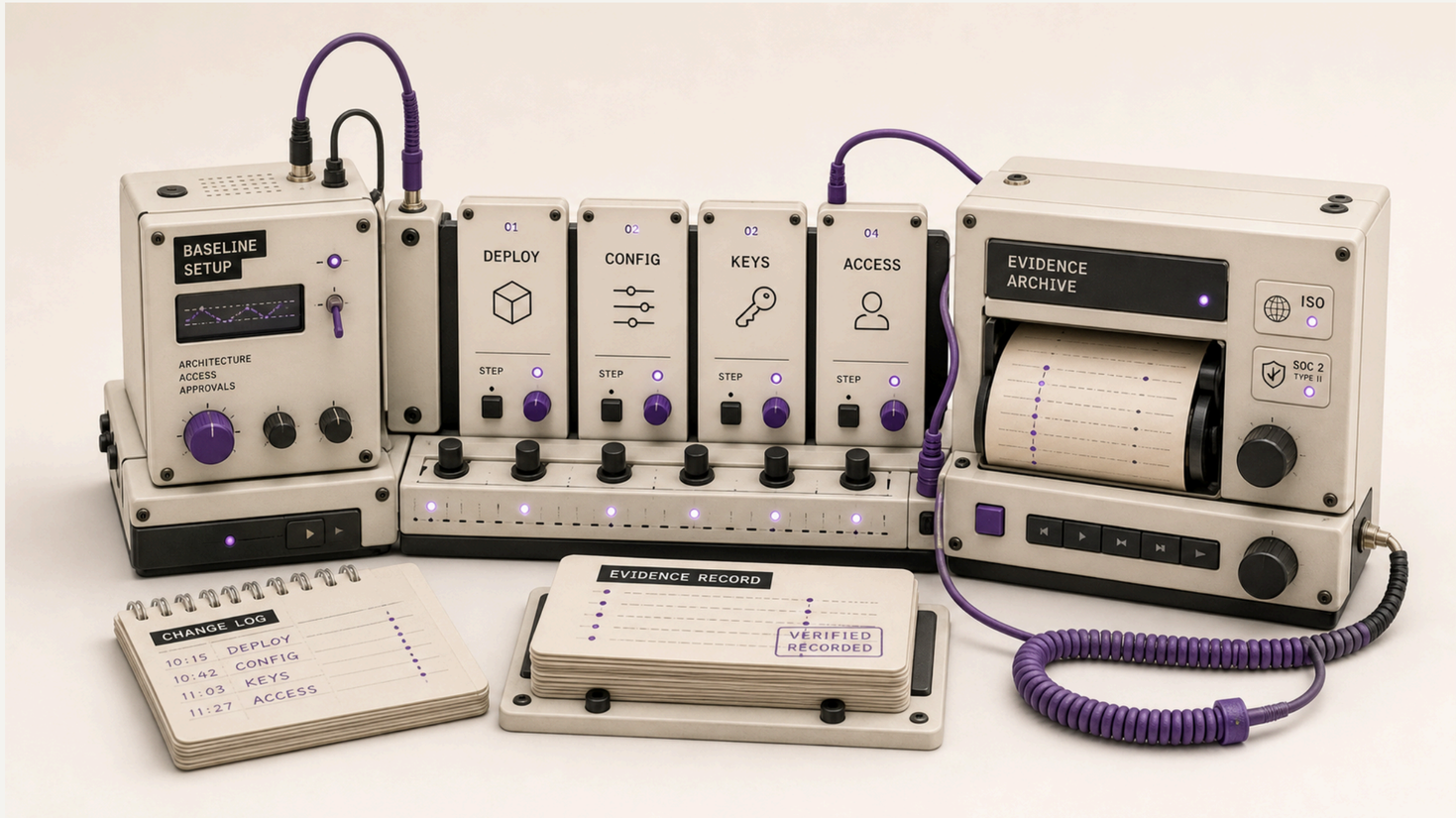
How long can you attest, replay, and defend the record?

Compliant operations

01 **Baseline**
architecture, initial access, approvals

02 **Changes**
deploys, config, keys, permissions

03 **Evidence**
Gateway ISO and SOC 2 Type II require the record



0:00 +0:00

Business continuity

FORK

Open source

Audit the box.

EVM

Standard stack

Solidity, JSON-RPC,
Foundry.

EXIT

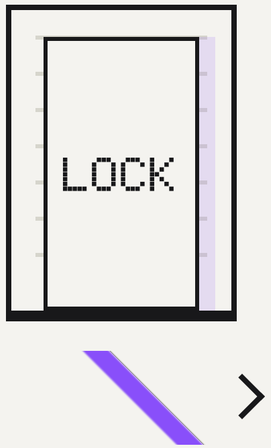
Continuity

No business hostage.

Cost of mistakes

ONE-WAY DOOR

CANNOT RE-ENCRYPT

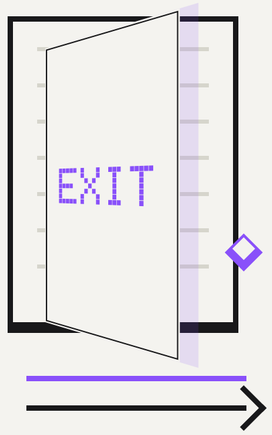


CANNOT ROLL BACK

On-chain ciphertext, irreversible disclosure, or private state with no migration path.

TWO-WAY DOOR

ROTATE KEYS



MIGRATE / RECOVER

Off-chain data, private chains, RBAC, key rotation, re-encryption, rollback and recovery paths.

Zcash Orchard A privacy bug can make recovery and verification the expensive part.

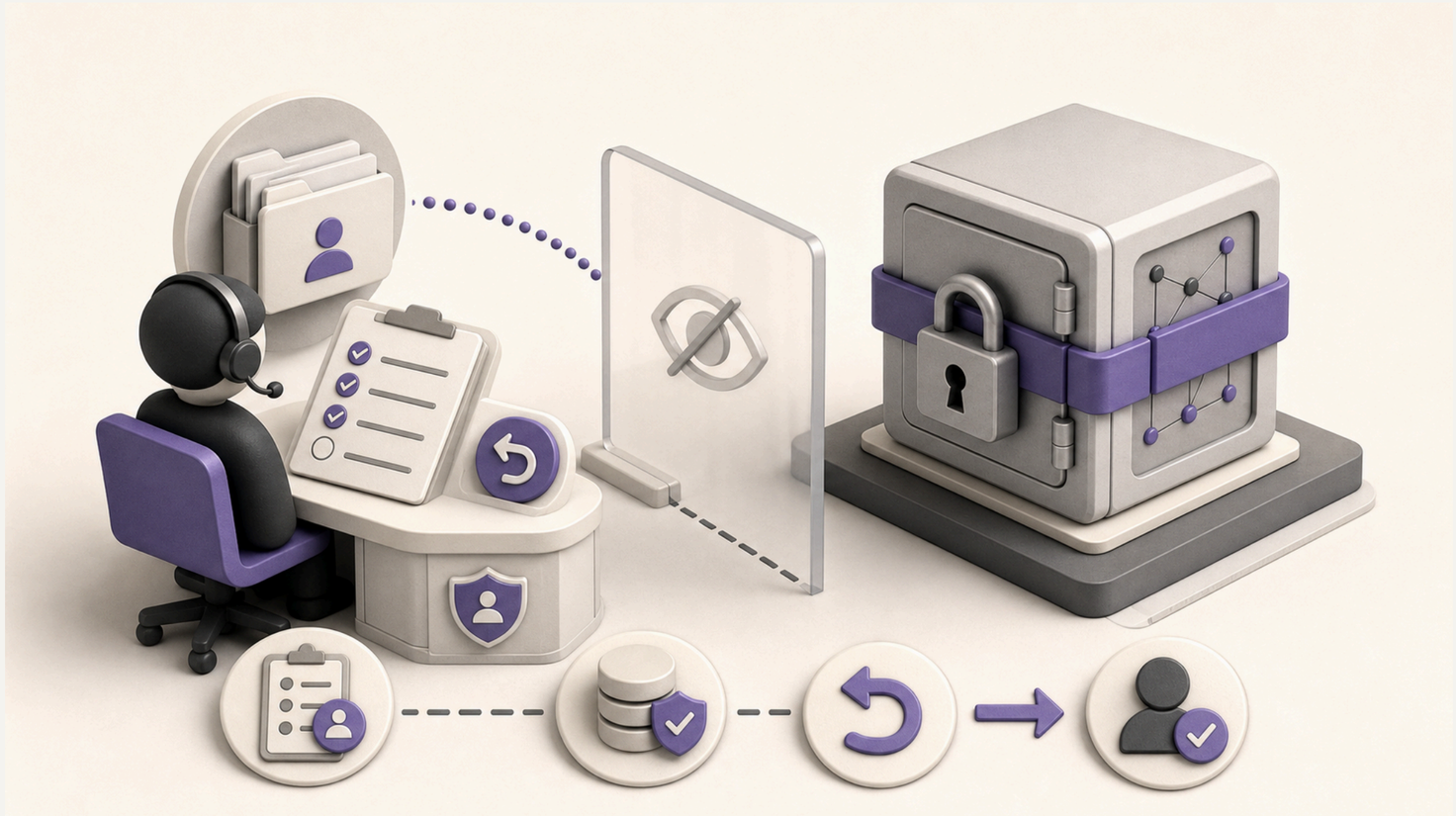
Disaster recovery

01 **Key loss recovery**
who can restore access, and under what controls?

02 **Data recovery**
can private state be restored, replayed, or migrated?

03 **Rollback paths**
can the system undo, re-issue, or contain damage?

04 **Customer support**
full privacy can make some support actions impossible



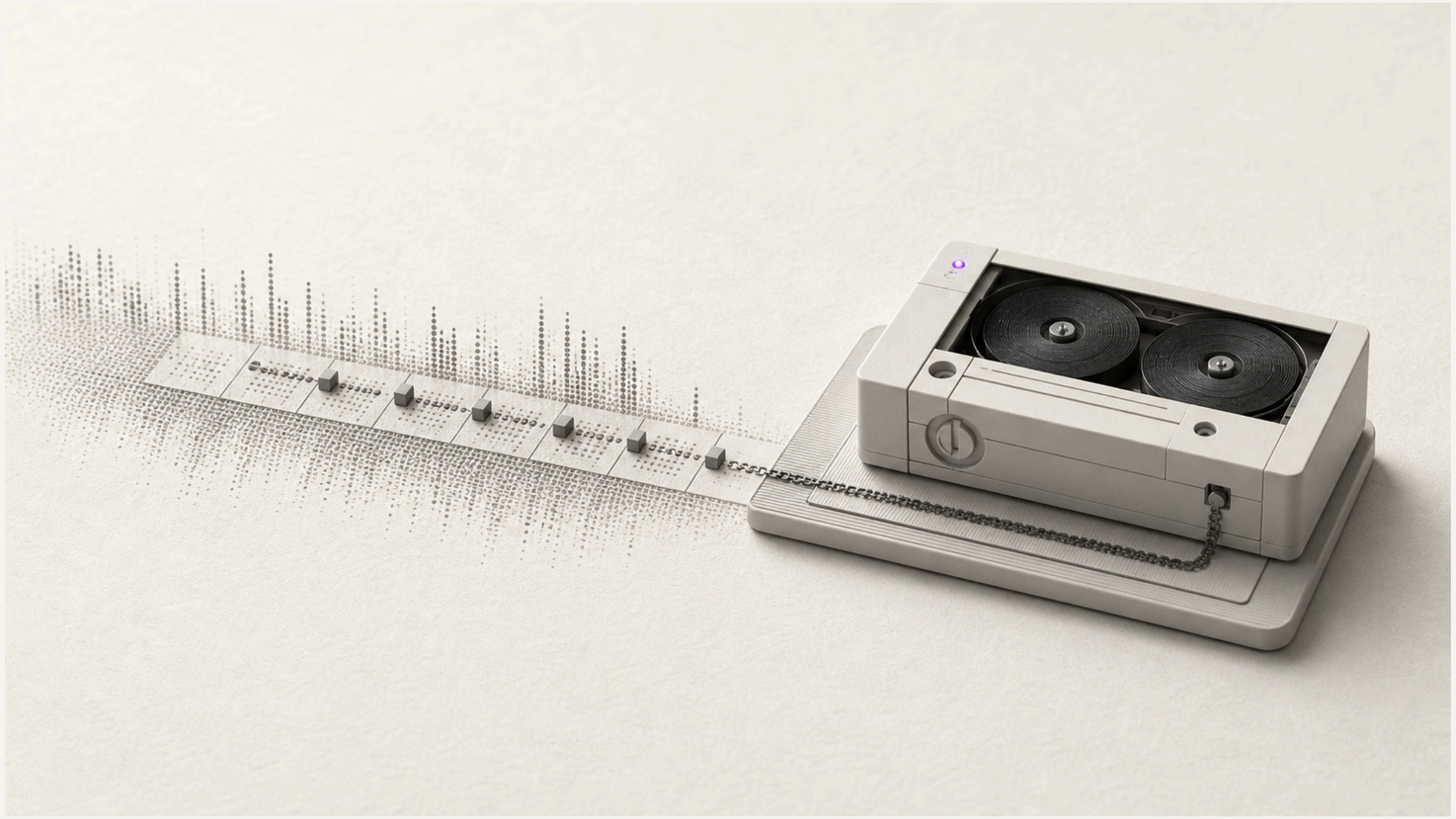
0:00 +0:00

Ciphertext is forever

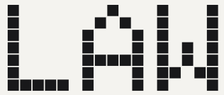
01 **On-chain crypto**
permanent ciphertext you cannot re-encrypt

02 **Post-quantum**
harvest now, decrypt later becomes a planning item

03 **Off-chain / RBAC**
rotate, re-encrypt, or avoid ciphertext in that layer



Legal risk



Applicable laws

Privacy, AML, sanctions, market abuse, Travel Rule, jurisdictional gray areas.



Fines + lawsuits

Caps, multipliers, claims, reporting clocks, remediation duties.

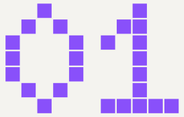


Gray areas

Gray areas and legislation conflicts.

0:00 +0:00

Operator privacy



Is it needed?

If the operator must not see user state, private state needs somewhere to live and recover.



Sometimes yes

Advanced crypto, or designs like Miden, can support it.



Not automatic

Even ZK or FHE systems may not provide operator-private state.



Complicated engineering

Storage, recovery, migration, audit, and support become part of the privacy design.

0:00 +0:00

Data provenance



Public chain

Anyone can download and analyze it, even ciphertext.



Privacy zone

Can it stay entirely on the customer's ground?



On premises

Private chain and telemetry stay on premises; Gateway can keep even telemetry there.

0:00 +0:00

Can you share just enough?



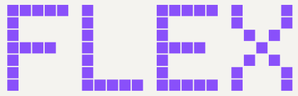
Who is asking?

Participant, counterparty, auditor, regulator, operator.



How much?

Only the fields, time range, and transactions they need.



Can setup change?

New roles, desks, jurisdictions, exceptions, emergency access.

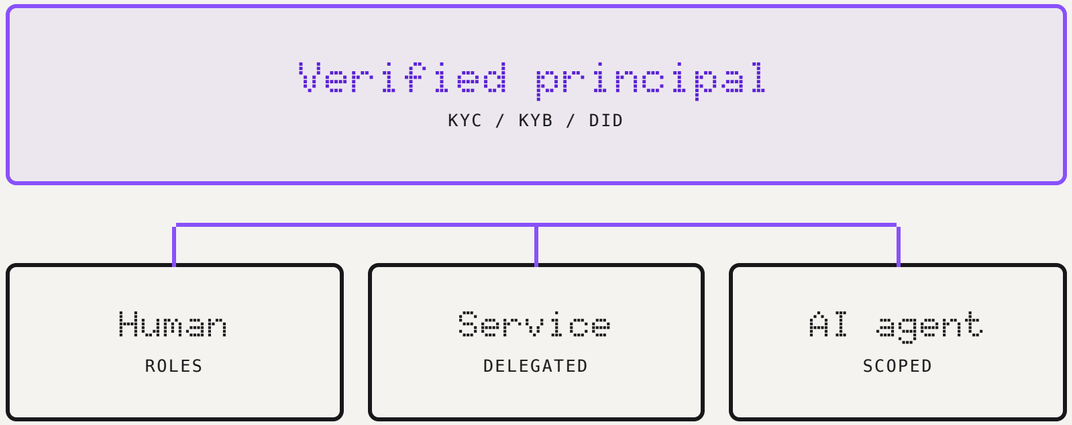
Blockchain of wallets vs blockchain of identities

WALLET CHAIN



BEARER INSTRUMENTS. WHOEVER CONTROLS THE KEY CONTROLS ACCESS.

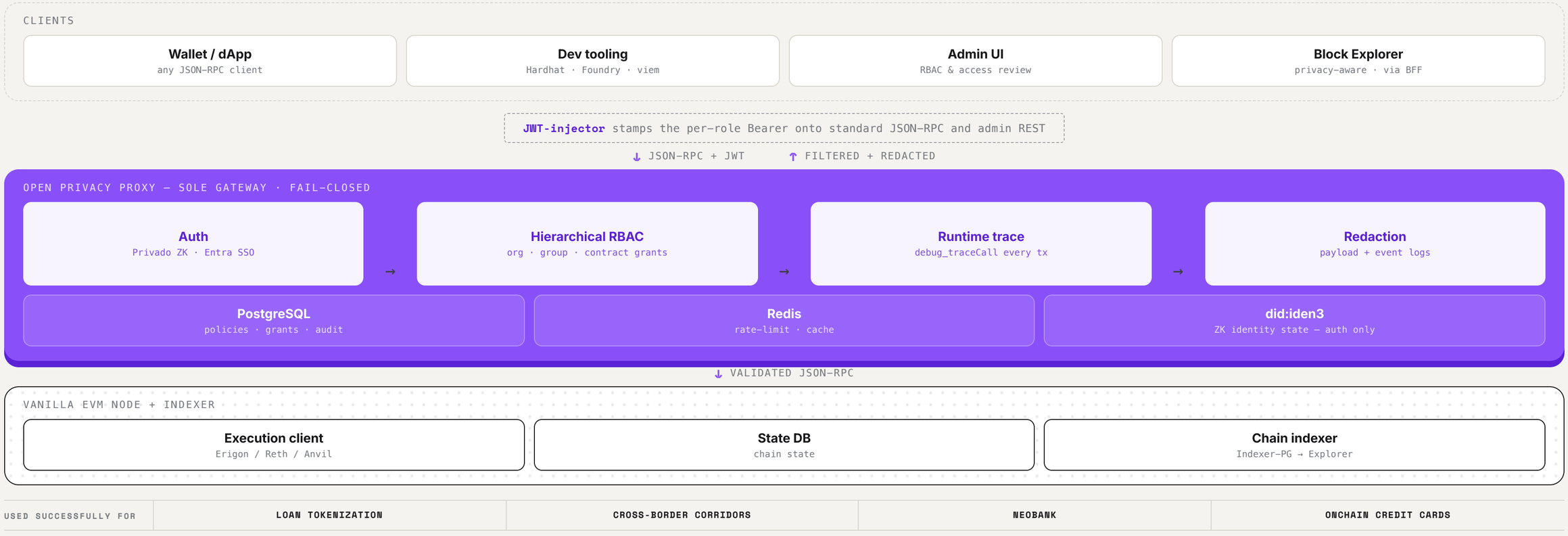
IDENTITY CHAIN



GOVERNED PRINCIPALS. ROLES, DELEGATION, REVOCATION, AND AUDIT LIVE ABOVE THE ADDRESS.

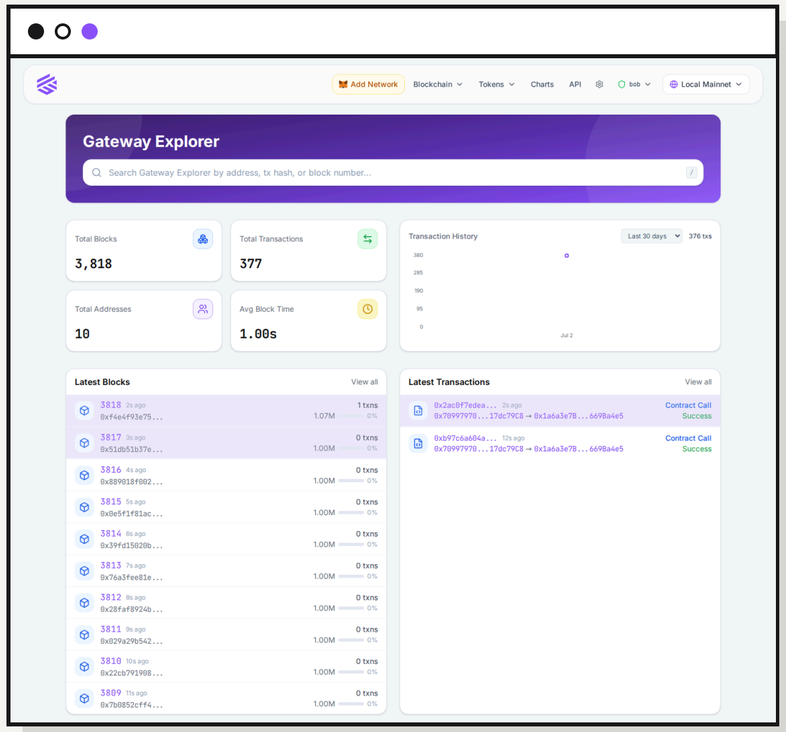
0:00 +0:00

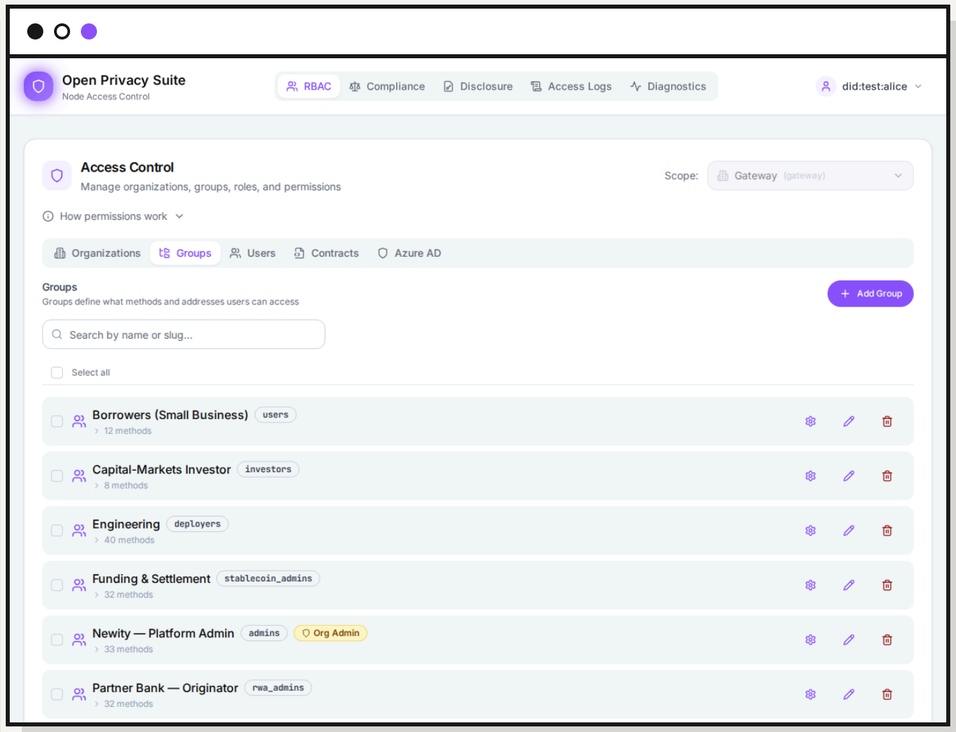
Architecture & components

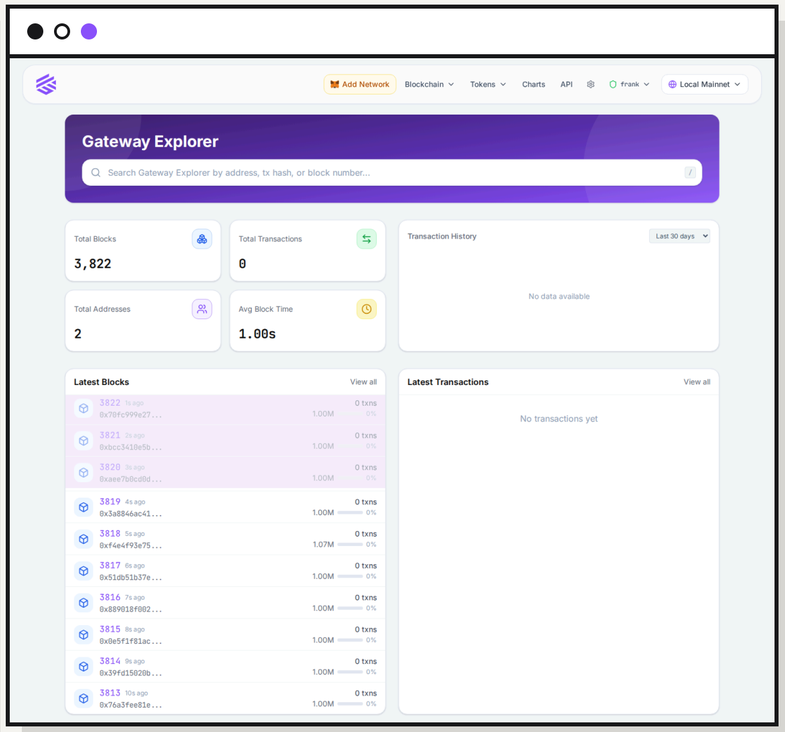


USED SUCCESSFULLY FOR	LOAN TOKENIZATION	CROSS-BORDER CORRIDORS	NEOBANK	ONCHAIN CREDIT CARDS

0:00 +0:00


Add Network
Blockchain
Tokens
Charts
API
bob
Local Mainnet
Gateway Explorer
Search Gateway Explorer by address, tx hash, or block number...
Total Blocks
3,818
Total Transactions
377
Transaction History
Last 30 days
376 txs
Total Addresses
10
Avg Block Time
1.00s
Latest Blocks
View all
Latest Transactions
View all


Open Privacy Suite
Node Access Control
RBAC
Compliance
Disclosure
Access Logs
Diagnostics
did:test:alice
Access Control
Manage organizations, groups, roles, and permissions
Scope:
Gateway (gateway)
How permissions work
Organizations
Groups
Users
Contracts
Azure AD
Groups
Groups define what methods and addresses users can access
Add Group
Search by name or slug...
Select all
Borrowers (Small Business)
users
12 methods
Capital-Markets Investor
investors
8 methods
Engineering
deployers
40 methods
Funding & Settlement
stablecoin_admins
32 methods
Newity — Platform Admin
admins
Org Admin
33 methods
Partner Bank — Originator
rwa_admins
32 methods


Add Network
Blockchain
Tokens
Charts
API
frank
Local Mainnet
Gateway Explorer
Search Gateway Explorer by address, tx hash, or block number...
Total Blocks
3,822
Total Transactions
0
Transaction History
Last 30 days
No data available
Total Addresses
2
Avg Block Time
1.00s
Latest Blocks
View all
Latest Transactions
View all
No transactions yet

0:00 +0:00

Open Privacy Suite

Open source

Apache-licensed reference implementation.

IaC install trails

Full-stack setup and changes from code.

Travel Rule
IVMS101 thresholds and workflows.

Sanctions
Real-time screening.

JWT Bearer
Rotated tokens.

Entra ID
Enterprise SSO.

did:iden3
ZK identity.

Existing tooling
Works with normal developer tools.

Existing tokens
Compatibility with live assets.

Hierarchical RBAC
Org, group, user, admin tiers.

Contracts
Per-contract grants.

Selectors
Function rules.

Parameters
Caller-bound guards.

Fail closed
Default deny.

Selective disclosure
Three visibility levels, time-bound requests.

RPC redaction
Payload filtering.

Logs
Receipts, blooms.

Traces
debug_trace filtering.

Audit hashchain
Tamper-evident log, SIEM webhook.

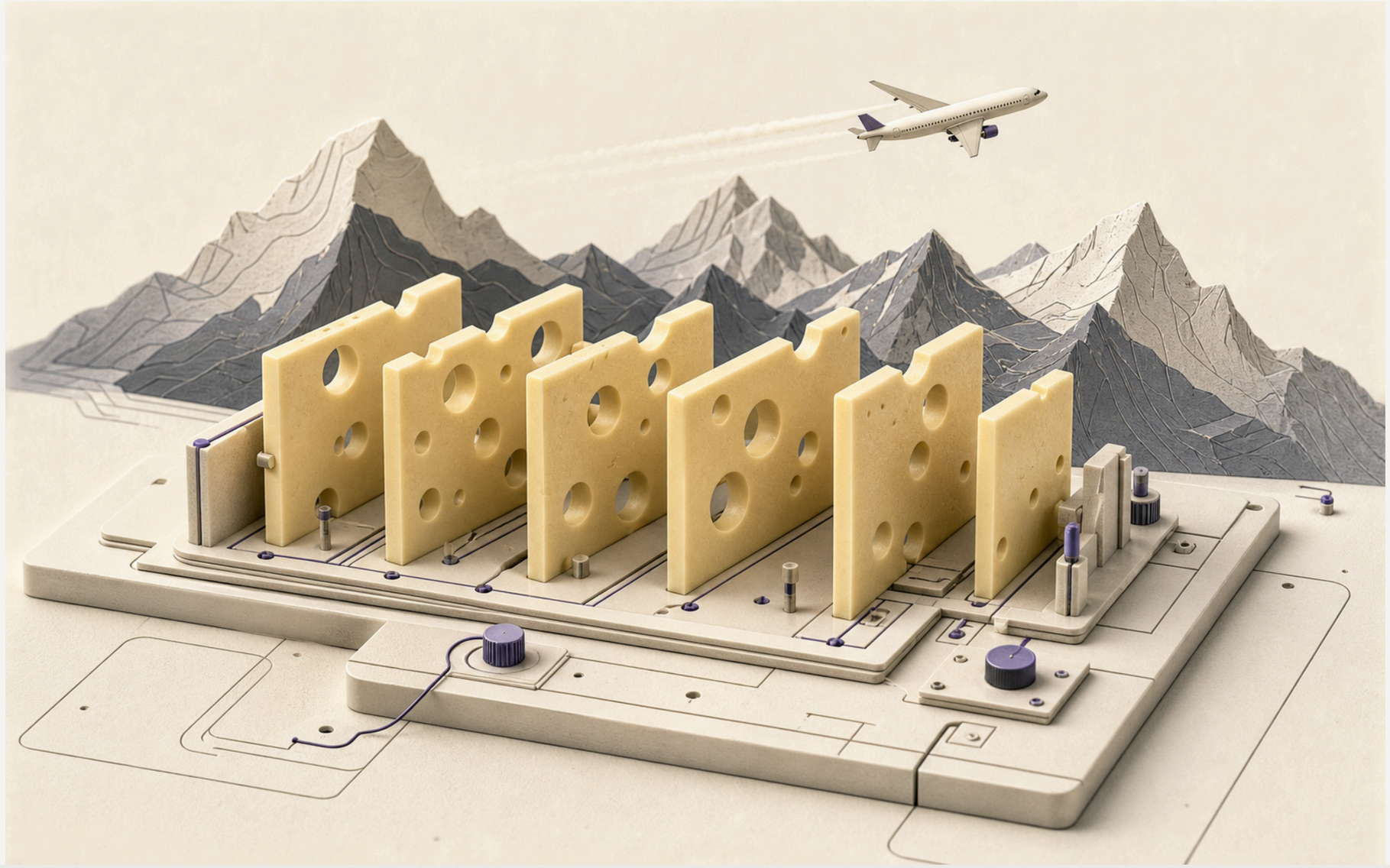
Consensus contribution
OPS input from Consensus work.

Tested stack
OP, CDK, Reth, Besu, Lineth.

Private-chain RBAC
Access control for private chains.

Privacy zones
Satellites for public chains.

0:00 +0:00



0:00 +0:00

Gateway

ISO/IEC 27001 | SOC 2 TYPE II
| GDPR-READY
| DATA SOVEREIGNTY

Digital asset infrastructure that abstracts complexity end to end.

CONTACT IGOR

igor@gateway.fm

EASY TO REACH

Selected work

2000+ L2s

provisioned

2x onchain cards

one live: **Gnosis Pay**

Ethereum PoS

transition work

Efficient validators

top-tier Ethereum operations

Stellar RPC

main RPC for **3+ years**

Miden stack

infra, explorer, AggLayer, stateless ZK proving

Guardian-as-a-service

institutional service model

Microsoft POCs

10x cheaper, 3x faster; SSI for agents and permissions

EY Nightfall

ran **4 dev environments** of the privacy rollup

OPS pilots

institutional privacy deployments

Payments + credit

cross-border remittance and loan tokenization pilots

Polygon core dev

zkEVM and CDK

Perps

with **Infinex**

Apex Group

chain / infra partnership

Reserve Bank of Australia

pilot infrastructure, with **Canvas**

Global failover

bare metal ⇄ public cloud, proven in practice

No-downtime migrations

private chains to L2s

0:00 +0:00