Programmable Privacy for EVM: A Deep Dive into Paladin

an LF Decentralized Trust Lab

Peter Broadhurst, Engineer & Co-Founder, Kaleido
Andrew Richardson, Engineer & Digital Assets Lead, Kaleido
March 5, 2025

LF DECENTRALIZED TRUST LABS

Agenda

1. Paladin client overview
2. Privacy models
3. Reference domains
4. Demo
5. Bringing it all together
6. Q&A

PALADIN

Programmable Privacy

LF DECENTRALIZED TRUST LABS

Privacy Frameworks

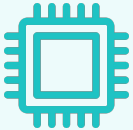
- **ZKP Tokens** — ZKP rules & custom logic
- **Issuer Backed Tokens** — EVM or off-chain notarization
- **Private EVM** — Any EVM Smart Contract
- *... next new privacy model on EVM*

Wallet Functions

Token & Contract APIs

Private Data Store

Key Management



ZKP Proof Engines

Client Functions

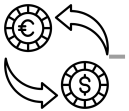
Transaction Orchestration

Indexing

Event streams

Encrypted Data Transfer

Existing (non-private) Tokens / Contracts



Atomic Swap Contracts

Privacy Preserving Smart Contracts

EVM

*no modifications necessary

Node Registry

PALADIN Runtime

HTTPS | JSON / RPC | WebSockets

Txns | Keys | States | Registry | ...

Embedded UI

Transaction Engine

Base Ledger Submission Engine

- Nonce Management
- Gas Price Management
- Signing
- Submission

Event-driven Engine

Private Submission Engine

- Assembly / Reassembly
- Coordinator selection
- Endorsement
- State distribution

Transaction store | ABI store | Transaction Management | Prepared Txn store | Status & Debug

Node Registry

EVM Backed | ...

Private Transports

MTLS + HTTPS | ...

Key Management & Signing

- Key mapping: Names | Paths
- Key deviation: HD | Direct
- Key storage: Local | HSM

Remote Signing Modules

Privacy Domains

Private EVM

Pente

- Full EVM
- Privacy Groups

besu

Notarized tokens

Noto

- Code notary
- EVM notary

ZKP backed tokens

Zeto

- Circom
- Nullifiers

WA WEBASSEMBLY

Blockchain Indexer

Block / Txns Events | Confirmations | Event Streams

Private State store

Reliable (DB) Storage | ABI based Schemas | Rich indexed query

Unmodified EVM

Base ledger EVM Contracts | *Atomic Swaps* | Public (ERC-20 etc.) | Privacy Group | Notarized Token | ZKP Token

Privacy Models

How Paladin Works

Business Workflows

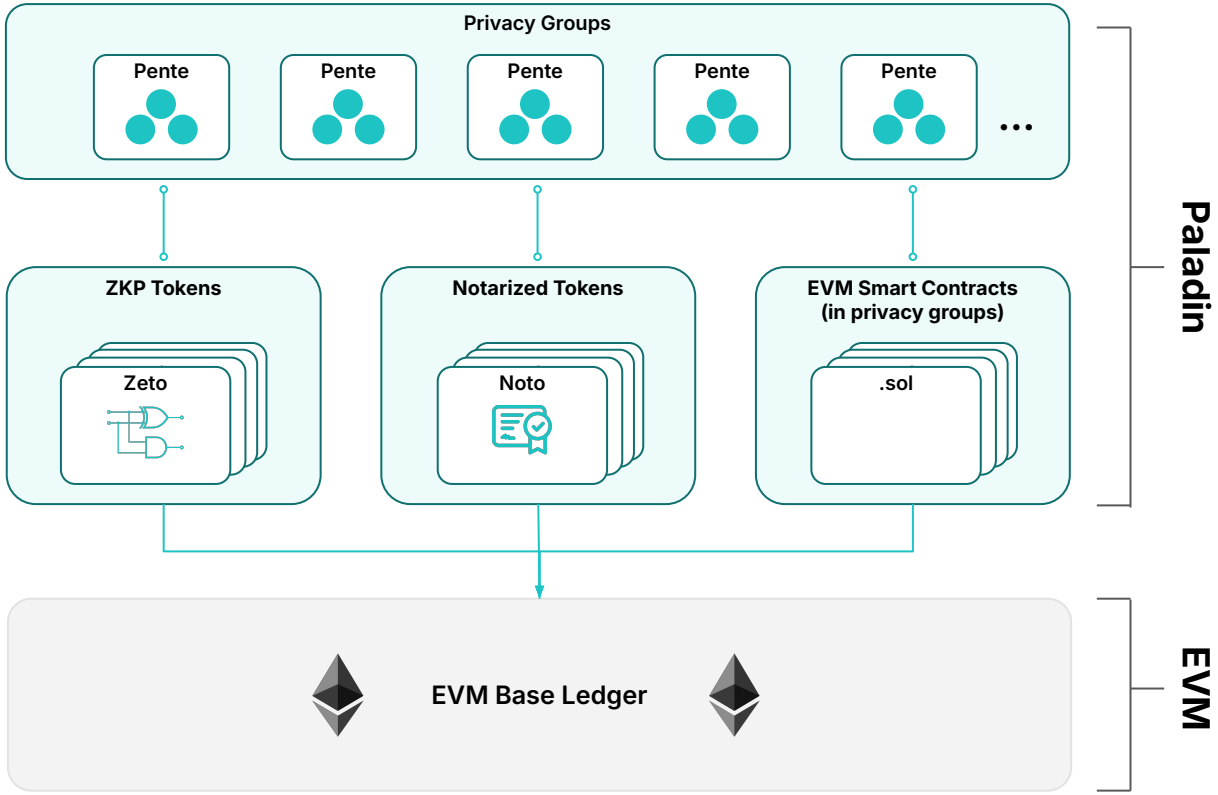
Utilize Pente privacy groups for approved parties to create and execute business logic.

Transaction Privacy

Utilize Zeto/Noto privacy preserving tokens or EVM Smart Contracts in privacy groups to execute confidential value transfer.

Global State

Record private transaction in shared global state while masking transaction details.

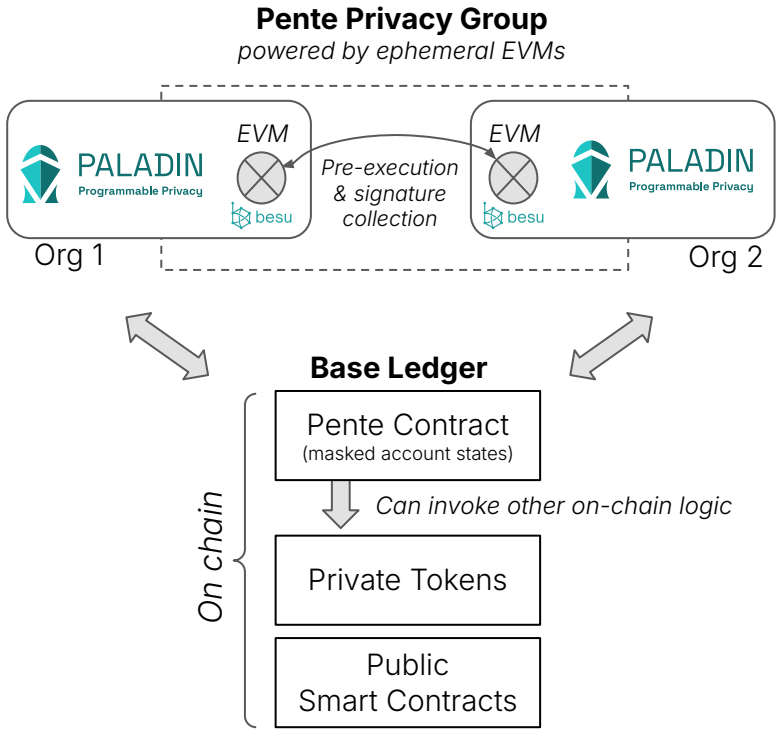


EVM Private Smart Contracts

Privacy Groups provide an EVM native way to program private workflows

The Pente Domain

- A Paladin Client can instantiate a *Pente Domain* to participate in privacy group workflows
- Pente improves on the architecture of prior Privacy Groups
- Developer friendly and simple to use
- Scalable & efficient design horizontally manages many parallel privacy groups



Pente Privacy Groups

- Each Org transacting in a Privacy Group runs an ephemeral EVM
- A Privacy Group EVM only runs to process a transaction (like Lambda)
- Endorsement signatures are collected and transactions submitted to the base ledger
- The base ledger enforces the inputs, outputs and order of every transaction

Token Privacy Models

*For privacy preserving tokens on a **shared ledger***

Paladin Token Domains

A Paladin ***Domain*** is a complete, full-stack implementation of a privacy architecture.

Orgs can play one or more roles within a domain.

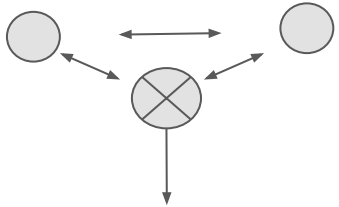
Noto and Zeto are extensible reference domains provided out of the box.

A single Paladin client can belong to many domains.

In the future there may be more domains supported by Paladin.

Issuer Backed Private Tokens

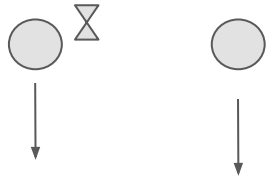
Ref implementation: **Noto**



A trusted party manages all state off chain and signs a transaction pre-submission.

Zero Knowledge Private Tokens

Ref implementation: **Zeto**



All parties maintain state off chain. One or more parties generate proofs for transactions that go on chain.

ZRC-20
ZRC-721

Help me choose!

There are many relevant factors to weigh when choosing including:

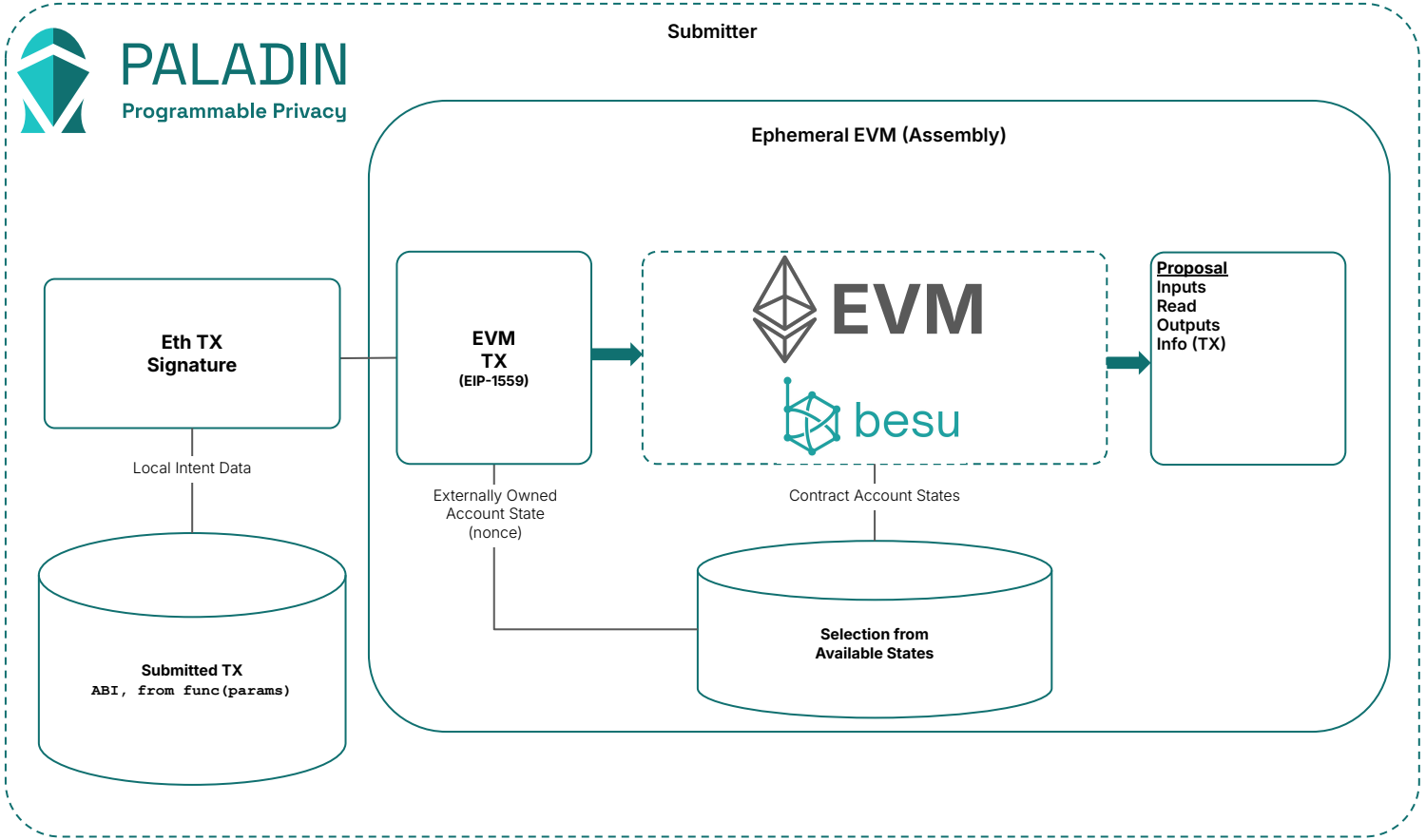
- Regulation
- KYC/AML needs
- Audit responsibility
- Trust model
- Throughput
- Compute cost
- Tech maturity

... and it isn't strictly one or the other.

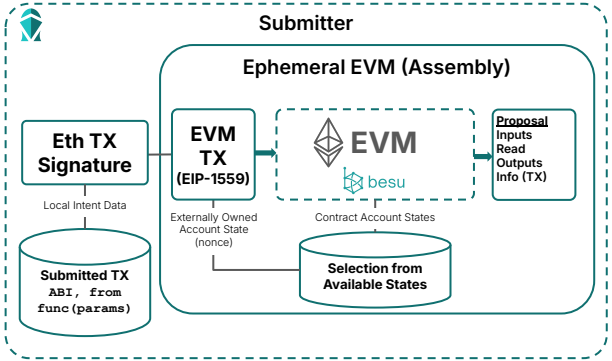
Example: Governance activities like issuance and KYC/AML might be issuer-backed, and simple trades might be fully decentralized via ZKP

Reference Domains

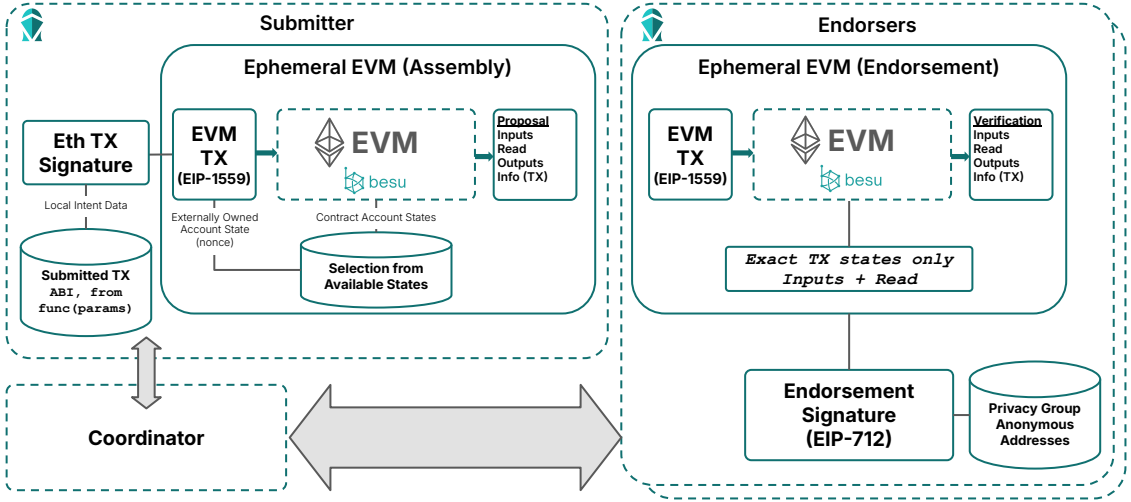
Pente EVM Privacy Groups: ASSEMBLY



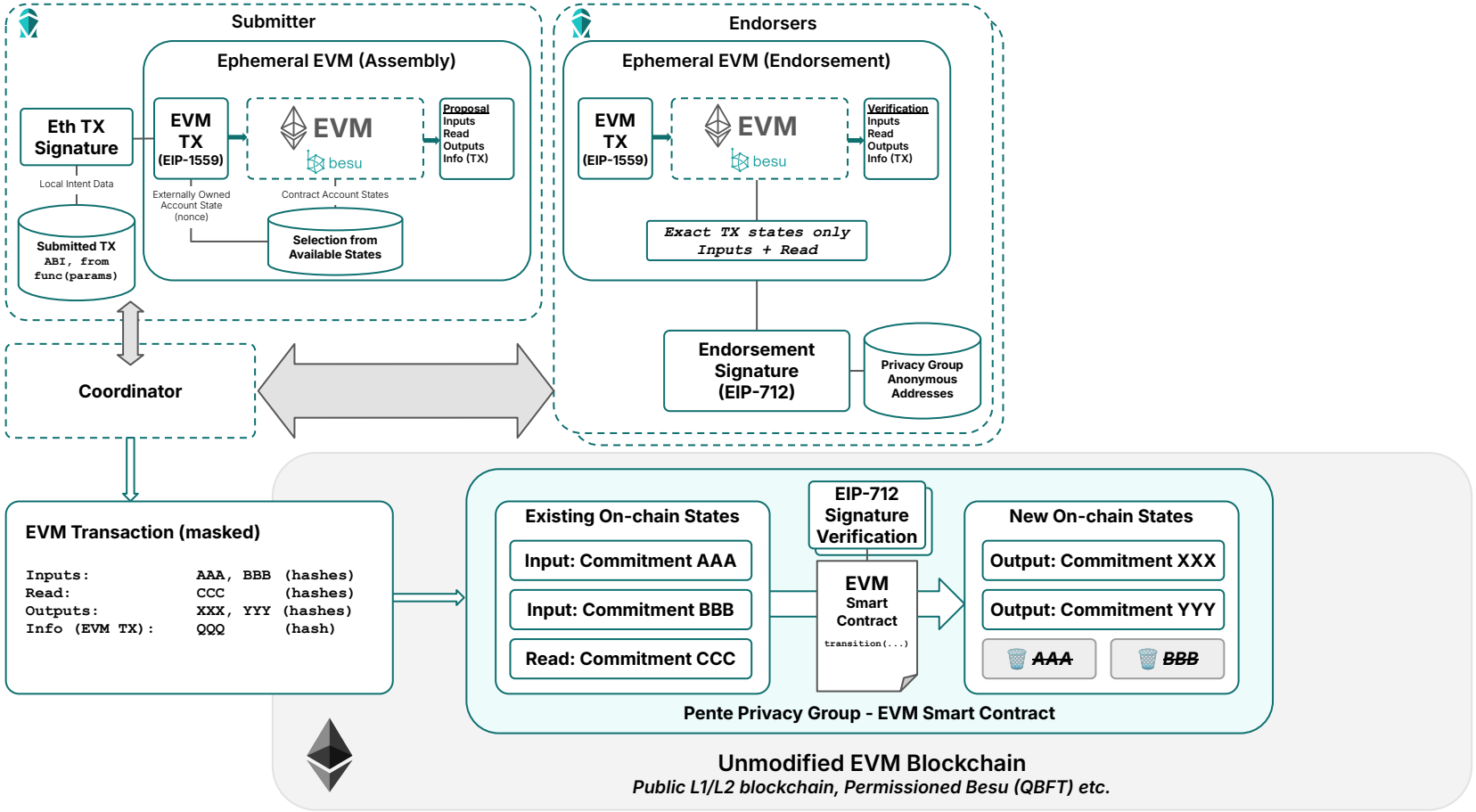
Pente EVM Privacy Groups: ASSEMBLY



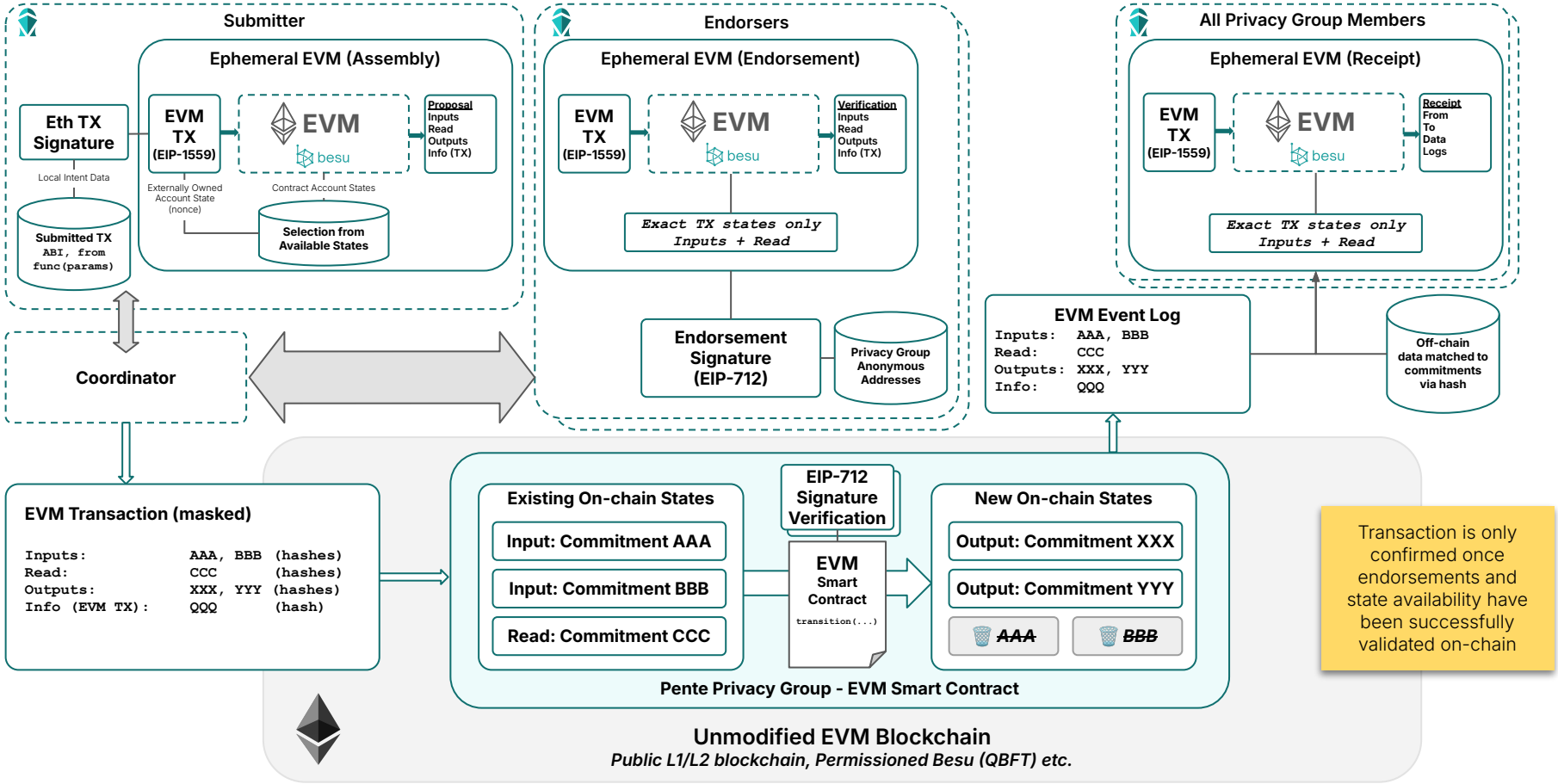
Pente EVM Privacy Groups: ENDORSEMENT



Pente EVM Privacy Groups: SUBMISSION



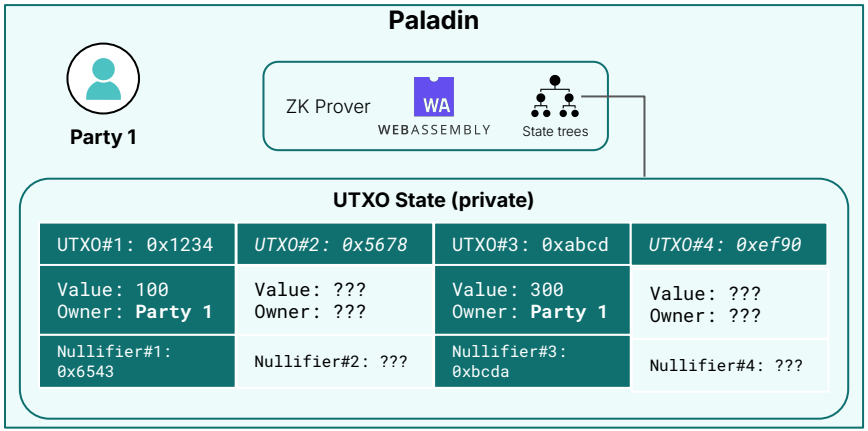
Pente EVM Privacy Groups: CONFIRMATION

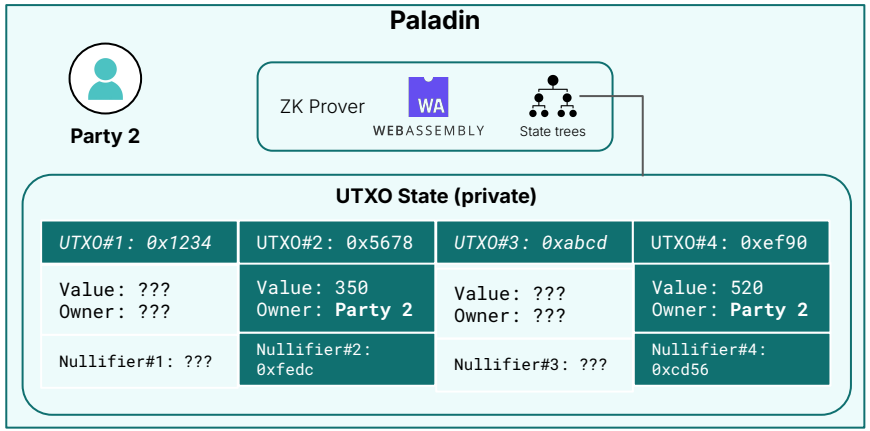


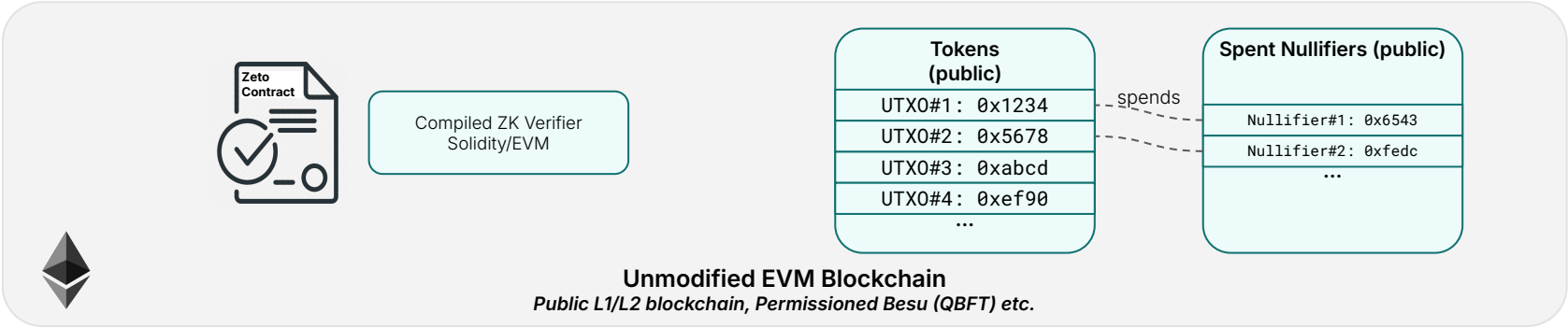
Transaction is only confirmed once endorsements and state availability have been successfully validated on-chain

Zeto: ZKP Backed Tokens

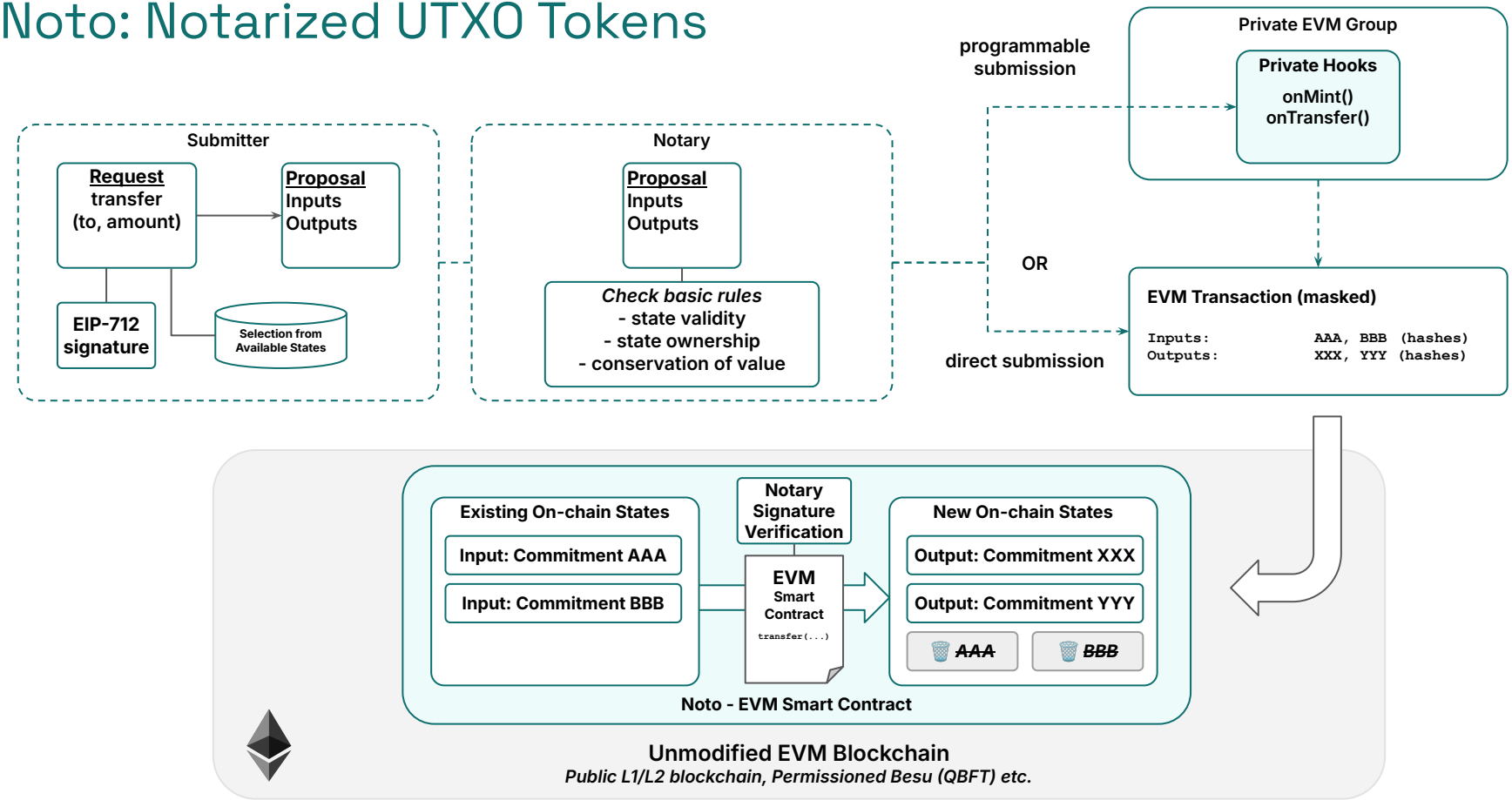
Using **Commitments** to represent the token economy, and **Zero Knowledge Proofs** to enforce transaction processing rules. The Paladin client maintains private states on behalf of the users. The blockchain verifies the proofs.





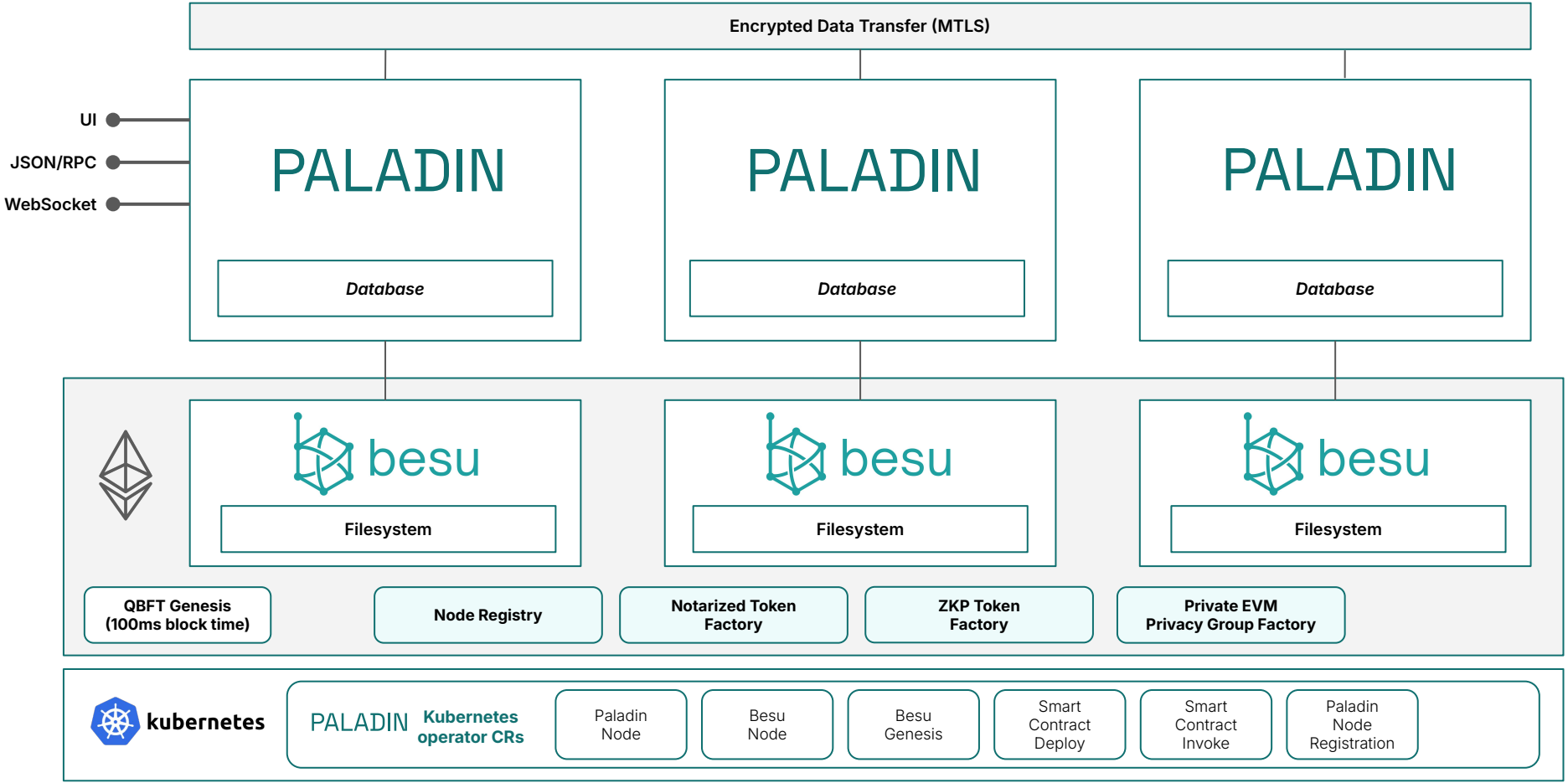


Noto: Notarized UTXO Tokens



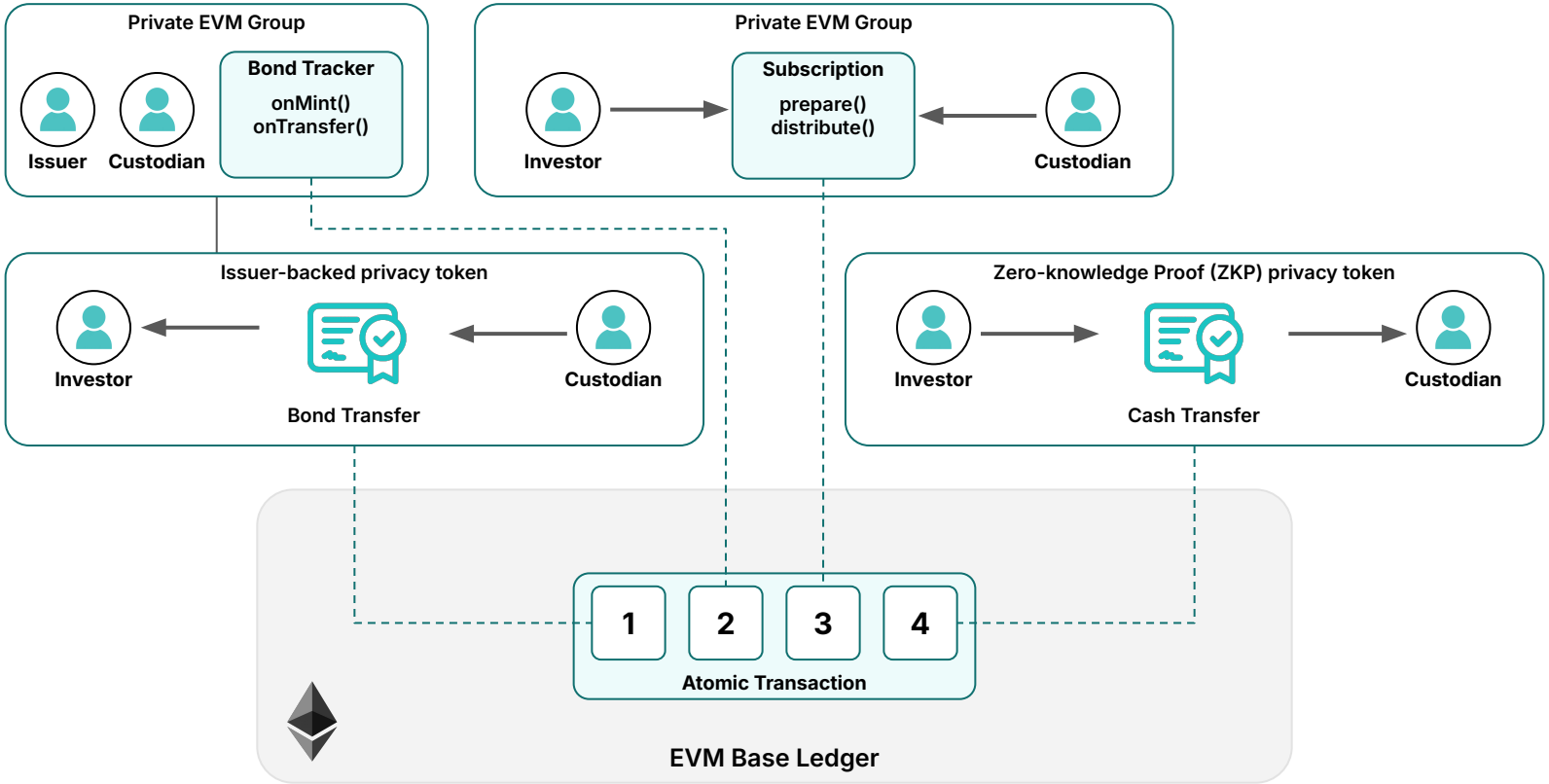
Demo Time

Paladin Deployment Automation: Get Running in Minutes



Bringing It All Together

Atomic DvP with Sub-Transaction Privacy



Paladin delivers programmable, composable Atomic DvP across the entire privacy stack

Q&A

Get all the links at:
https://www.paladinprivacy.org/

PALADIN
Programmable Privacy

LF DECENTRALIZED TRUST LABS

Privacy Frameworks

- **ZKP Tokens** — ZKP rules & custom logic
- **Issuer Backed Tokens** — EVM or off-chain notarization
- **Private EVM** — Any EVM Smart Contract
- *... next new privacy model on EVM*

Wallet Functions

- Token & Contract APIs
- Private Data Store
- Key Management
- ZKP Proof Engines

Client Functions

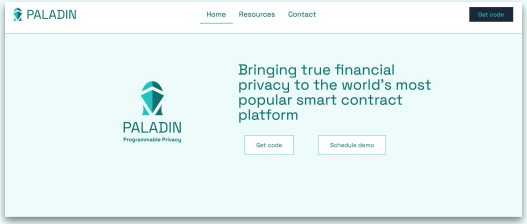
- Transaction Orchestration
- Indexing
- Event streams
- Encrypted Data Transfer

- Existing (non-private) Tokens / Contracts
- Atomic Swap Contracts
- Privacy Preserving Smart Contracts
- EVM *no modifications necessary
- Node Registry

How To Get Involved

Get the code and sign up to receive updates at paladinprivacy.org.

Join the community



By registering for updates on paladinprivacy.org, you'll get exclusive invites to in-person privacy workshops.

You can also start a conversation with the maintainers by joining the Discord.

Read more

To learn more about the lab, check out Peter and Andrew's technical overview of Paladin on the LF Decentralized Trust blog.

Request a briefing

kaleido

To talk with an expert about how Paladin can unlock your use case, schedule time with a Kaleido solution architect.