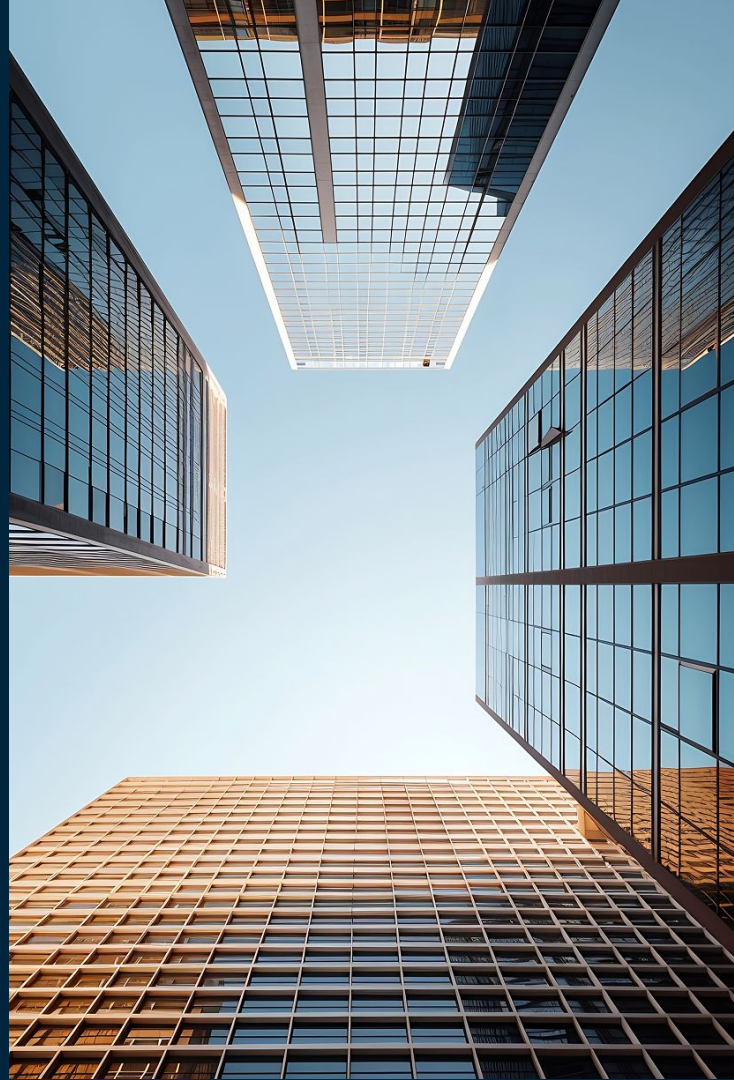
NETHERMIND

Compliant Privacy on Public Blockchains

Stefano De Angelis - Lead Researcher

LFDT Privacy Workshop - London, July 1th 2026



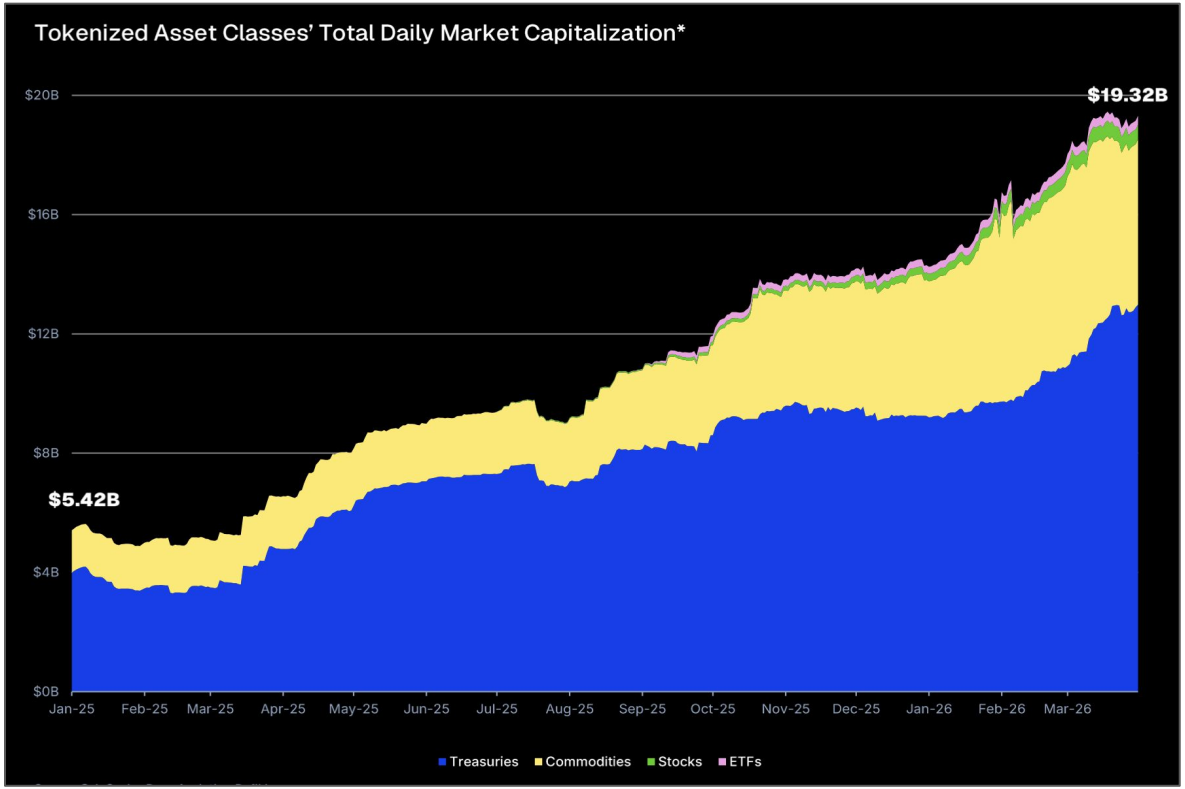
Public blockchains are **transparent** and **immutable** distributed ledgers replicated over a permissionless set of peers

The Problem

Transparency on Public Blockchains

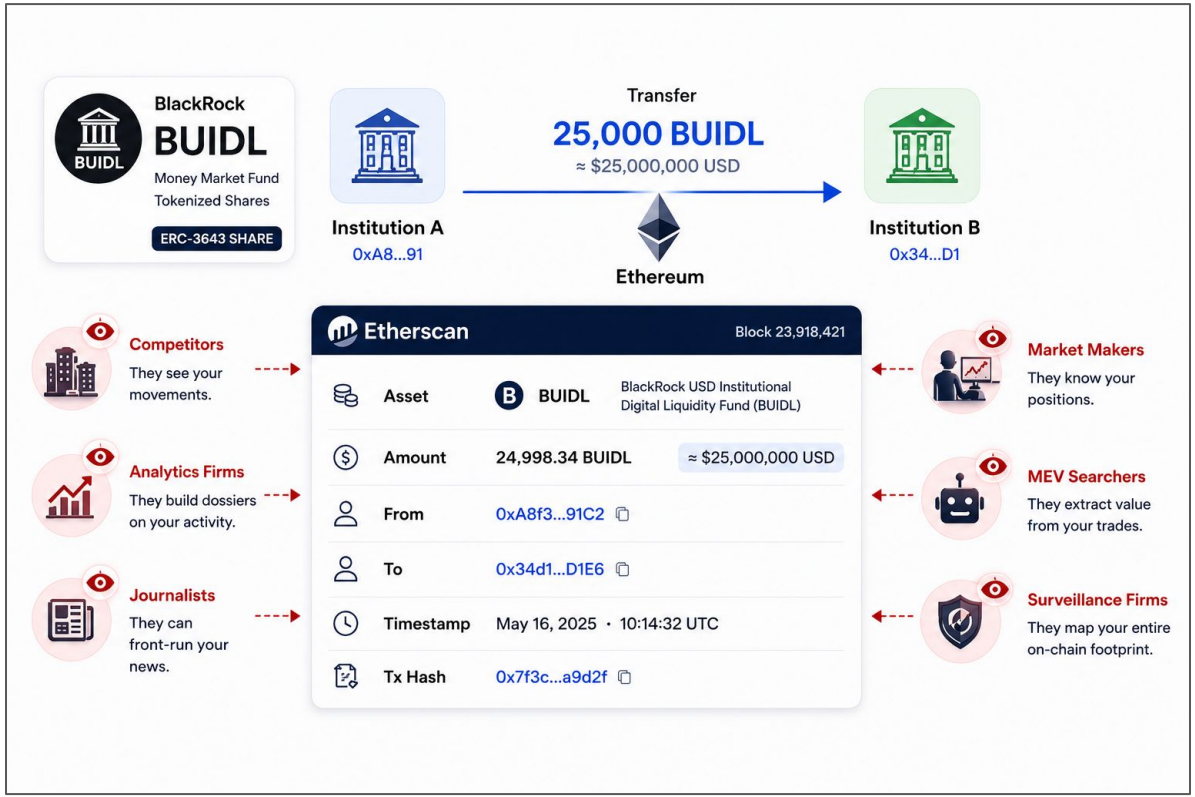


Adoption is Growing



CoinGeko 2026 RWA Report

Real World Scenario



Full Transparency Exposes Sensitive Data



Transparency

Financial assets residing on public blockchains, such as treasury bonds, deposits, and stocks, are fully visible to the outside world.



Positions & Balances

Asset holdings, investor balances, and bank treasuries are all stored transparently and are easily observable.



Settlement Exposure

Real-time public observability exists for the sender and receiver counterparties involved in financial trades, asset exchanges, and payments.

On-chain Privacy is the Moat

- Privacy is an **obstacle for global finance** adoption
- Money flows, treasuries, strategies, and counterparties can't be leaked



Existing approaches and their limitations

Cryptographic techniques and their applications for privacy-aware services on public chains

Private Transfers

Commonly realized with **shielded pools**. Use of **zero knowledge proofs** and encrypted notes in a **UTXO-based state tree**. Broadly adopted in smart contract applications (e.g. Tornado Cash) and well established L1s (e.g. ZCash).

Sailoed smart contract (pools); lack interoperability and standardization; limited compliance features.

Example: Railgun, Privacy Pools

FHE / MPC

Fully-Homomorphic Encryption (FHE) enables computation on encrypted data. **Multi-Party Computation (MPC)** unlocks computation over confidential states.

*FHE is computationally intense and not battle tested technology. Stability and efficiency are main challenges. FHE and MPC operate under **trust assumption** for encryption/decryption keys.*

Example: Zama, TACEO

Validiums

Private chains that maintain a **private state off-chain** and only publish commitments and zk-proofs on public layer. **RBAC** used for privacy and compliance.

*Expensive computation on **zkVMs**, **closed environments** with managed infrastructure.*

Example: Prividium (zkSync)

Two main challenges

Privacy

Balances, transfers, treasuries and counterparties are trivially observable on public ledgers. Any sensitive financial data becomes reconstructable. This is not acceptable for financial institutions and represents both a financial and regulatory risk.

Compliance

Institutions operate under AML/CFT obligations, sanctions regimes, reporting requirements, and internal governance controls that are designed around accountability.

Regulated entities cannot bypass compliance in favour of confidentiality. Fully obfuscated information flows and anonymized data sets are not acceptable.

Our Solution

Compliant Privacy for Public Blockchains



A unified privacy layer for regulated financial assets

Compliance and Standardization

Ethereum standards like ERC-3643, ERC-1400 bring together **tokenization with compliance** controls and identity management.

Confidentiality and Interoperability

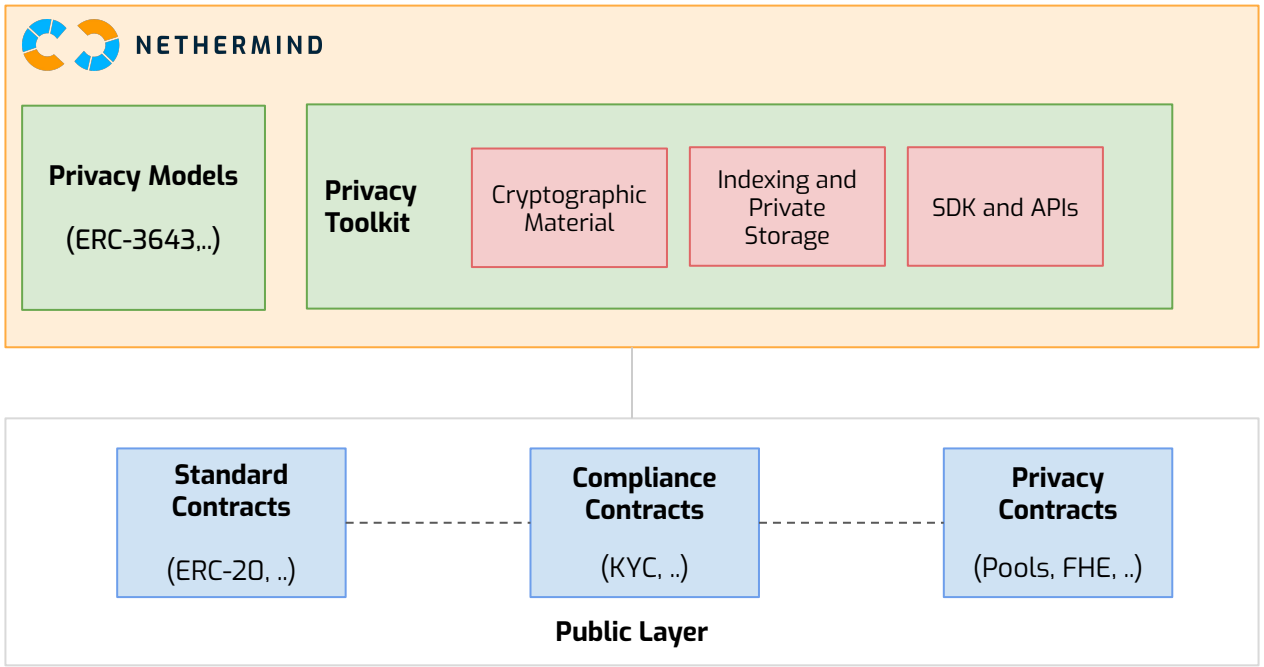
Combine permissioned token standards with confidentiality guarantees by still leveraging the **same base public layer.**

Private Transfers

Use cryptographic protocols to ensure **transactions validity**, **compliance controls** and avoid siloed infrastructures.

By combining **privacy guarantees** with **native compliance**, financial institutions can transition to public blockchain infrastructure unlocking global liquidity while fully **protecting transaction data and comply with regulatory rules**.

Vision: Privacy Layer for Public Chains



Components requirements and characteristics



Privacy Model

Implementation of **standardized templates** that integrate with existing token standard on public ledgers. Use defined models, such as UTXOs, FHE, and private VMs.



Privacy Tools

Necessary **tooling** components for the interaction with the public layer. Manage **cryptographic material** like encryption keys and proof mechanisms; store **private states** and **index data** from the public layer.



SDK and APIs

Provide the **interfaces** to consume and integrate privacy solutions at the application level. Hide complexities related to privacy protocols facilitating adoption into **legacy systems**.



Base Layer

Adopt an integrated solution where privacy models are directly deployed on a **public base layer** (e.g. Ethereum), where assets and liquidity live.

Paladin Framework

EVM Programmable privacy

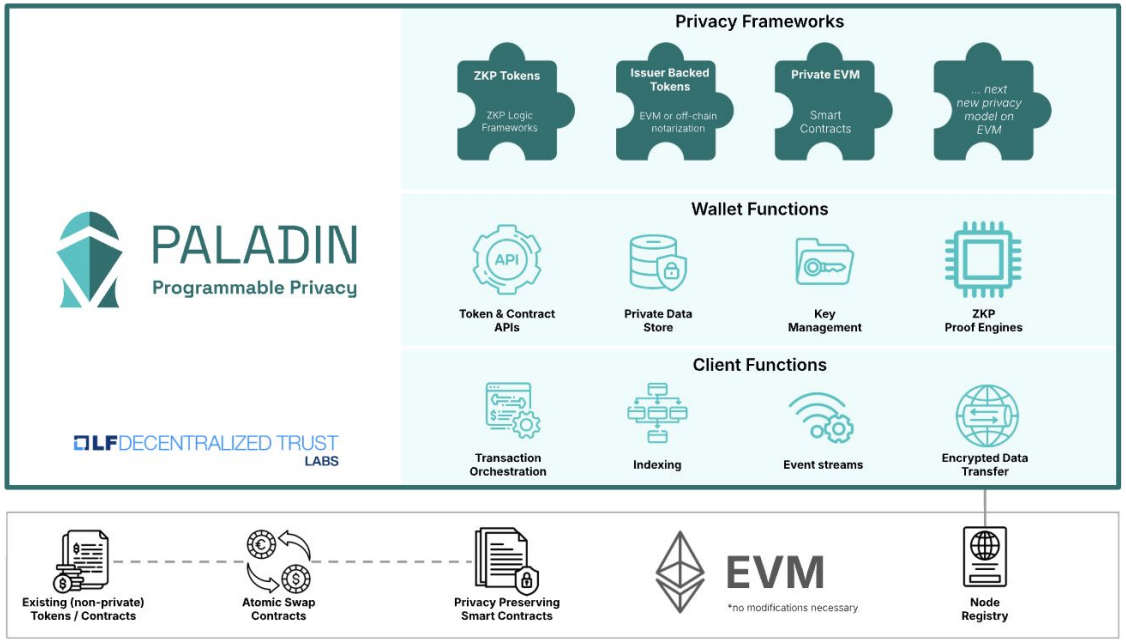
Full-stack solution

Private tokens templates

Modular and expandable

Privacy tooling available

Open source



Source: https://lfdt-paladin.github.io/paladin/head/

From vision to practice

A Tokenized Private Bond with Compliance

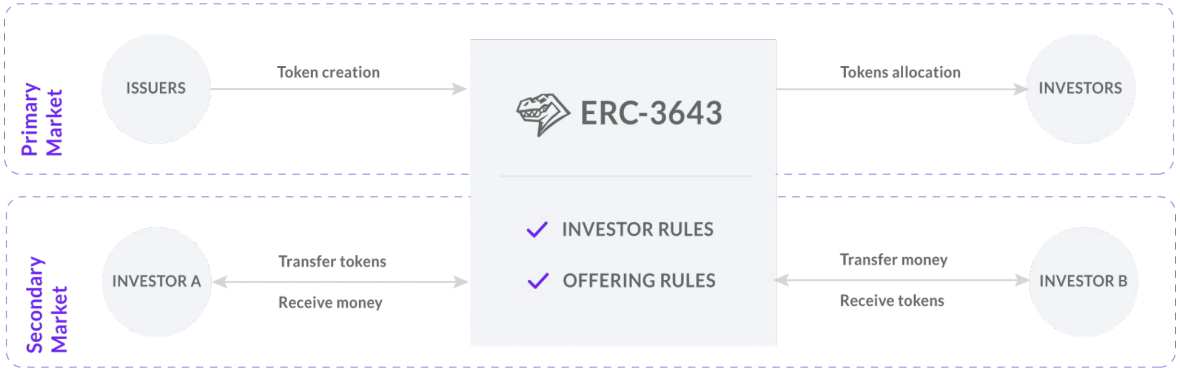


A real use case: ERC-3643

Practical instantiation of the unified privacy layer for permissioned assets on public ledgers.

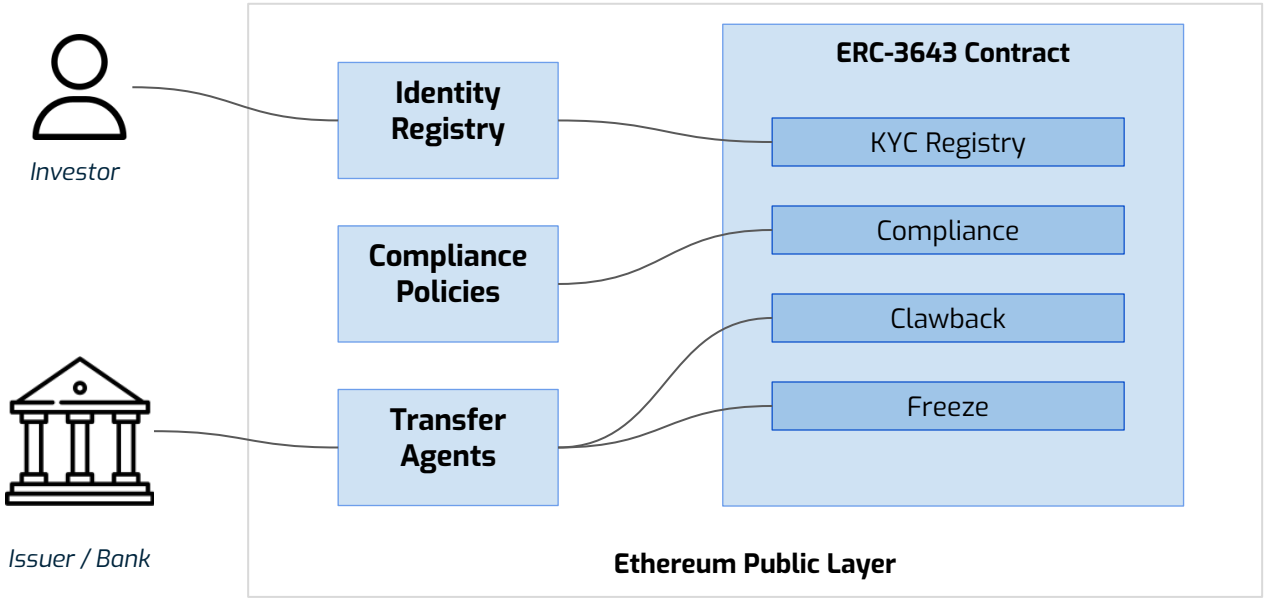
Proof of Concept with **ERC-3643** assets.

Standard for permissioned security tokens with compliance control.

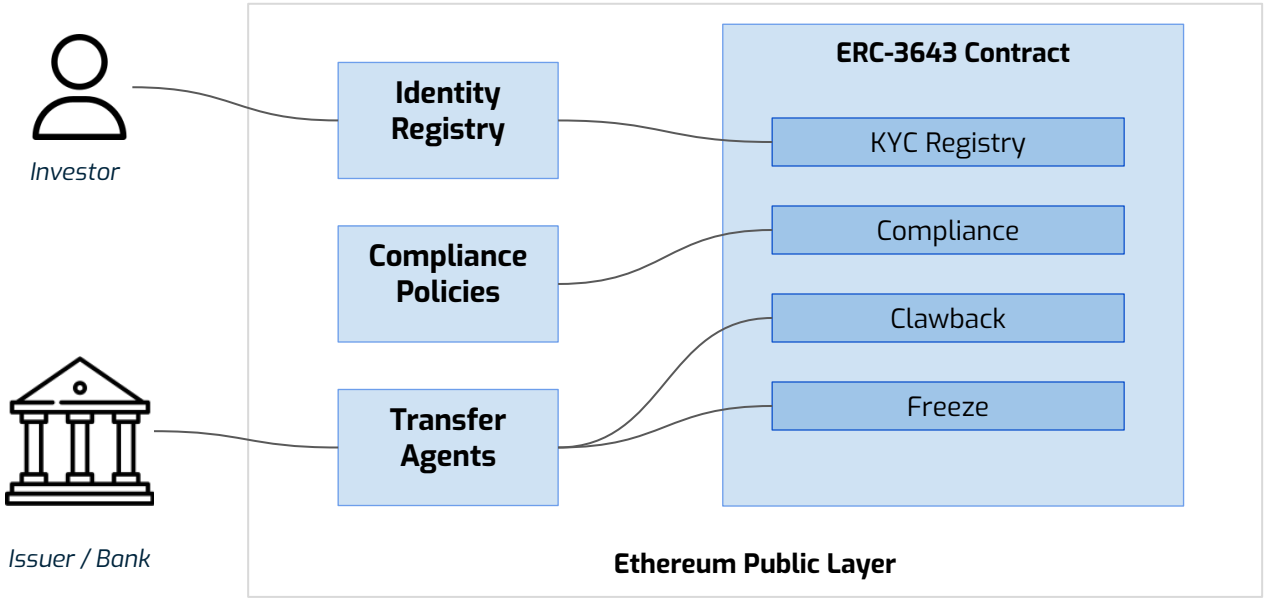


Source: https://tokeny.com/erc3643/

The ERC-3643 Standard

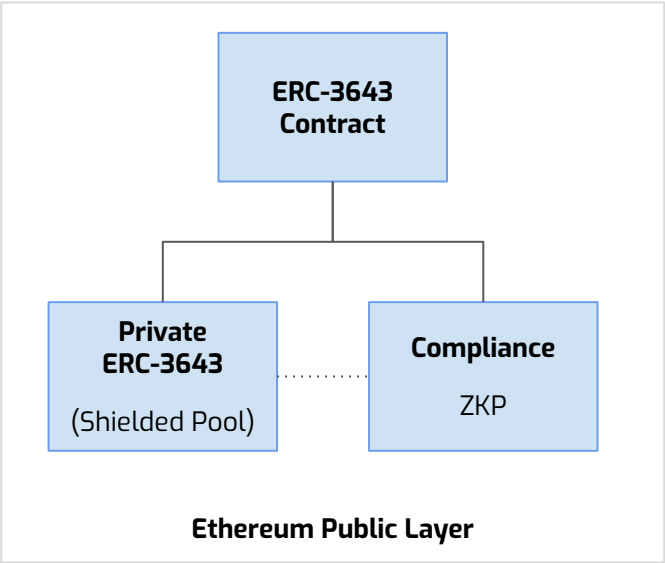


The ERC-3643 Standard



All the information is publicly visible on-chain

Privacy vs Compliance Challenge



ERC-3643 provides compliance but **lacks privacy**

Two Challenges:

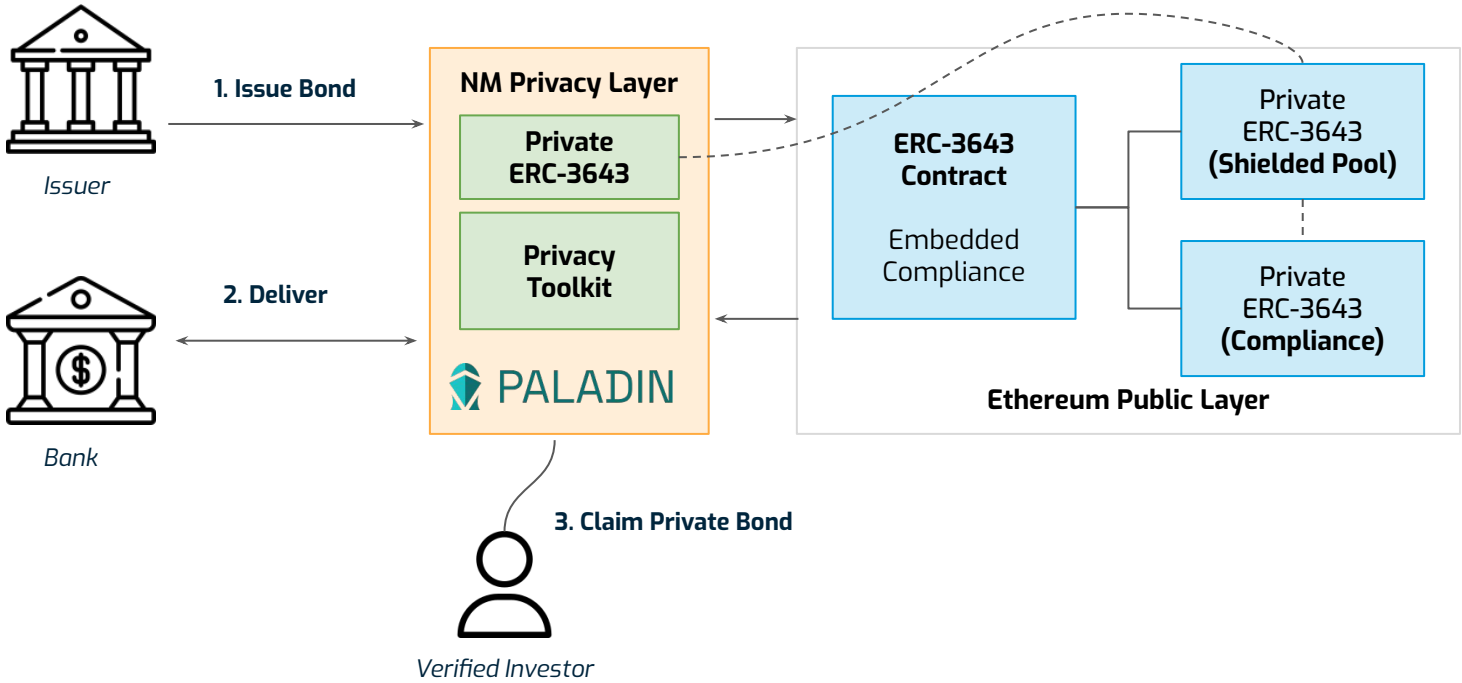
1. Build a private version of ERC-3643
2. Bring compliance in private ERC-3643

Our Approach:

- **Privacy Contract:** Shielded pool
- **Compliance Contract:** ZKP

Our Approach for Private ERC-3643

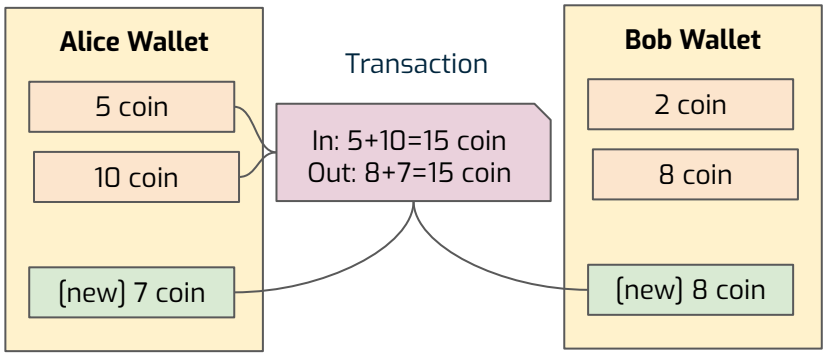
Issuance and distribution of a private bond



Privacy for ERC-3643



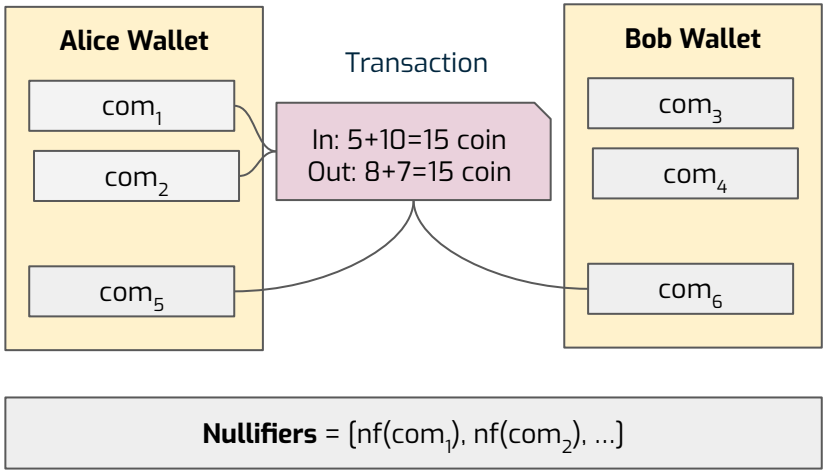
Privacy Contract: Shielded Pool



The UTXO model

A state model that holds assets and maintains a **UTXO-based** representation of asset ownership (i.e., **notes**), while enforcing correctness via on-chain ZK proof verification.

Privacy Contract: Shielded Pool

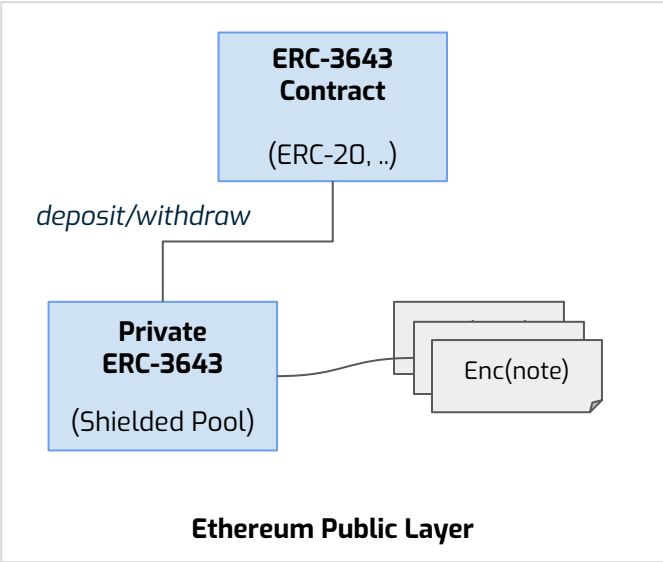


Privacy-preserving UTXO model

A “shielded domain” is an Ethereum smart contract that holds assets and maintains a **commitment-based** representation of asset ownership (i.e., **notes**) with Merkle Trees, while enforcing correctness via on-chain ZK proof verification.

- **User:** owns cryptographic identity
- **Notes:** only commitments + Merkle Root
- **Nullifiers:** list of spent notes
- **Proofs:** ZKP confirm validity

ERC-3643 Shielded Pool



Deposit, Transfers and Withdrawals

1. **Deposit** ERC-3643 tokens in the shielded pool contract
2. For every deposit create **encrypted notes**
3. Private UTXO **transfers** verified via **ZKP**
4. **Withdraw** back to ERC-3643

Visible on-chain:

Note commitments, nullifiers, proofs, encrypted notes

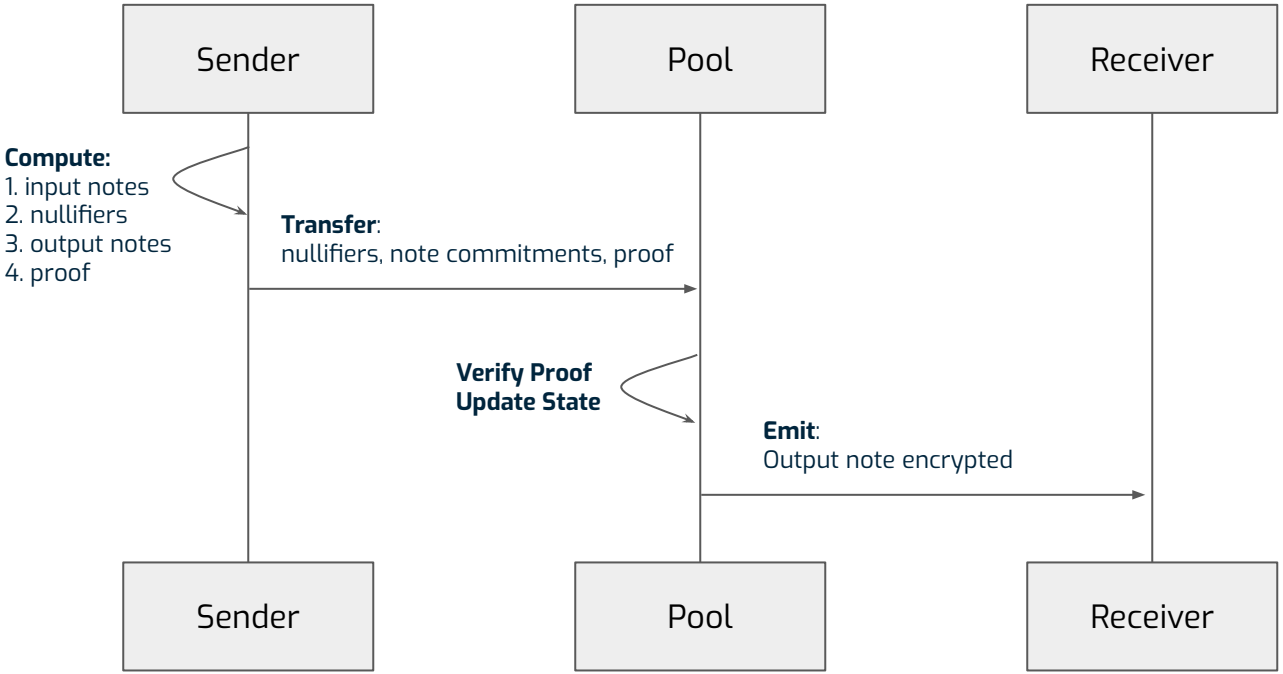
Confidential:

Notes: sender, receiver, amounts, balances

What ZK Proofs Verify

01	**Notes Ownership**	User is spending notes they own; for which they know a nullifier derived with a valid spending key.
02	**Note Existence**	The input notes exist in the pool's current note commitment tree (membership against the Merkle root).
03	**Value Conservation**	Amount of input and output notes are consistent (total input amount equals total output amount).
04	**Double Spending**	The spent note has not been nullified.

Transfer Flow



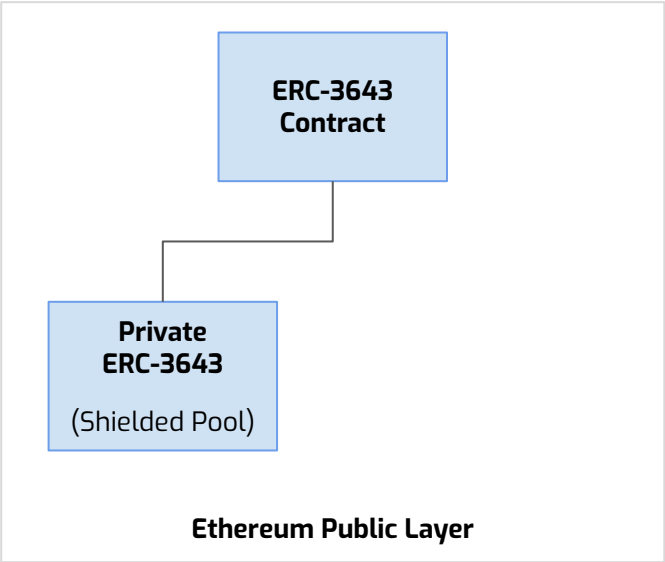
Advantages of the Shielded Pool Model

Native Compatibility	Integrates well with **ERC-20-based tokens**. No need to re-define new standards.
Public Chain Liquidity	Assets remain on public layer. **No fragmentation** across separate systems and avoids maintenance of additional infrastructures.
Practical & Scalable Privacy	UTXO with ZKP is a battle tested model. **Verification on-chain takes seconds** and **settles for under a dollar** making this model suitable for real-world financial transactions.
Privacy Without Trust	There are **no extra trust assumptions** apart from the soundness of the underlying proof system. Information remains confidential.

Compliance for Private ERC-3643

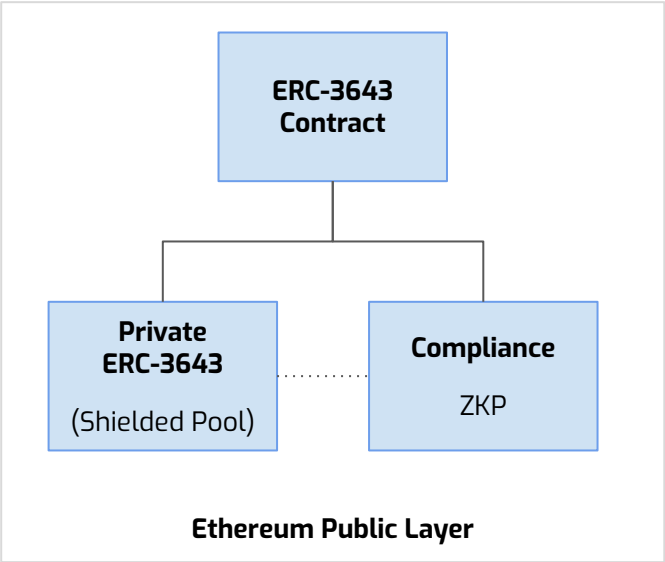


Compliance for Private ERC-3643



- Shielded Pools break ERC-3643 compliance
- Missing components:
  - **Selective Disclosure** for shielded transactions
  - **KYC authorization**
  - **Freeze** users
  - **Clawback** Assets

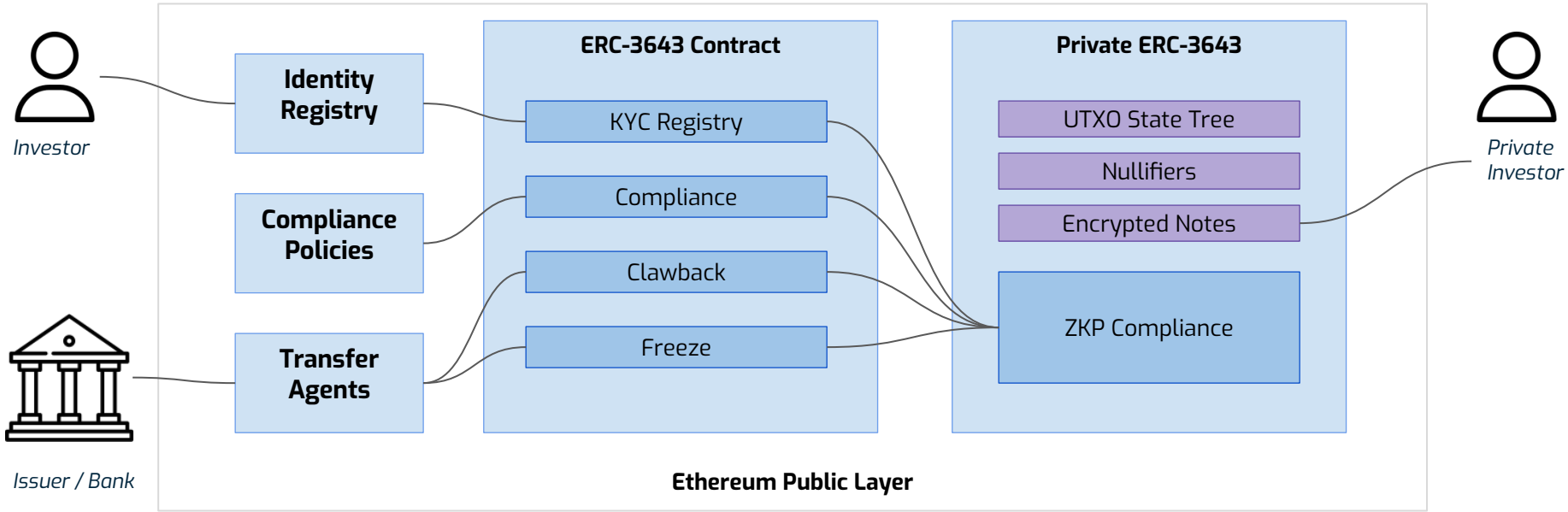
Compliance for Private ERC-3643



- Shielded Pools break ERC-3643 compliance
- Missing components:
  - **Selective Disclosure** for shielded transactions
  - **KYC authorization**
  - **Freeze** users
  - **Clawback** Assets

Solution: Compliance enforced with ZKP

The ERC-3643 Standard



Key Properties



Confidential Transactions

Asset balances, transfer amounts, transactions history, and counterparties remain confidential while still auditable.



Selective Disclosure

Regulators can access transactions data, KYC status and transactions history without revealing the information publicly.



Compliance Controls

Enable compliance controls that meet KYC requirements and asset controls for regulators and asset managers including account freeze and asset clawback.

Institutional finance can move on-chain enforcing regulatory rules without exposing sensitive data

NETHERMIND

Thank you

Stefano De Angelis

stefano@nethermind.io

@_deanstef

