Horizen Protocol

The Privacy Layer for the Base Blockchain

Horizen Labs Research
research@horizenlabs.io
v1.0.0 - Nov 13, 2025

Abstract

Horizen introduces a protocol for regulatory compliant, auditable privacy designed to complement the scalability and liquidity of Base, Ethereum's most active Layer 2. As activity and capital continue to concentrate on Base, the need for confidential yet verifiable execution has become critical for institutional and enterprise adoption.

The Horizen Protocol unifies two key components into a cohesive architecture for privacy-preserving computation: the Horizen Confidential Compute Environment (HCCE), which leverages Trusted Execution Environments (TEEs) for secure, attested computation, and the Horizen Chain, which enables state management and compliance-aware execution while maintaining Base-level composability and liquidity alignment.

Together, these components ensure that privacy flows with liquidity, extending Base's open execution model into a verifiable, compliance-ready framework for developers, institutions, and retail users. Horizen's approach bridges the divide between transparency and confidentiality, enabling a new generation of onchain applications that are secure, scalable, and regulation-aligned.

1. Introduction

1.1 The State of the Privacy and Scalability Market

In his 2024 essay *"The Three Transitions,"* Ethereum co-founder Vitalik Buterin outlined the three structural shifts required for Ethereum's long-term success: scalability through rollups, usability through smart-contract wallets, and privacy as a native protocol capability (Buterin, 2024). While the first two transitions have been substantially realized, **the third, privacy, remains the least developed and the most consequential.**

Ethereum's transparency has enabled an unprecedented standard of public verifiability, but it has also created a structural inhibition to institutional and enterprise adoption: every account balance and transaction is permanently visible. This model serves the ethos of trustless validation but **fails to accommodate the requirements of regulated finance, corporate operations, and privacy-sensitive users whose activities must remain confidential yet auditable.**

Recent advances in scalability have expanded Ethereum into a multi-layer ecosystem of rollups and execution environments. Among these, **Base** (Coinbase's Layer 2 network built on the OP Stack) has rapidly become Ethereum's execution arm. It hosts millions of daily transactions and a diverse application ecosystem spanning DeFi (Aerodrome, Uniswap v4 on Base), social protocols (Friend.tech, Base Name Service, Farcaster), and consumer apps (The Base App, Zora, mint.fun). This growth proves that Ethereum's scalability transition is functionally complete, but the privacy transition has not yet begun.

In September 2025, Base processed approximately **362 million** transactions (over **7.5 times** the **49 million** on Ethereum Mainnet ((BaseScan, 2025; Etherscan, 2025). By contrast, regulated private rails already operate at a massive scale. **JPM Coin**, running on J.P. Morgan's permissioned Quorum network, facilitates approximately US $1 billion in institutional transfers per day (Coindesk, 2023). **Kinexys Digital Assets** (J.P. Morgan's rebranded Onyx tokenization platform) has processed more than US $1.5 trillion in cumulative volume, with daily transaction averages exceeding US

$2 billion (BC-IFSA Journal, 2024). Meanwhile, the **People's Bank of China's e-CNY** has recorded over ¥7 trillion (≈ US $986 billion) in transactions since its launch (Central Banking, 2024). These figures illustrate that the constraint on institutional onchain adoption is no longer throughput or cost, but rather the **absence of compliant, auditable privacy**.

If translated to a public-chain equivalent, the existing institutional private-payment flows would correspond to an estimated **≈ 5 billion private transactions per month** - a conservative conversion assuming an average institutional transfer size of ≈ US $1,000 across the combined volumes of JPM Coin, Kinexys, and e-CNY (Horizen Labs Research, 2025). This "missing" layer of private, auditable transaction capacity defines the latent market opportunity for Horizen.

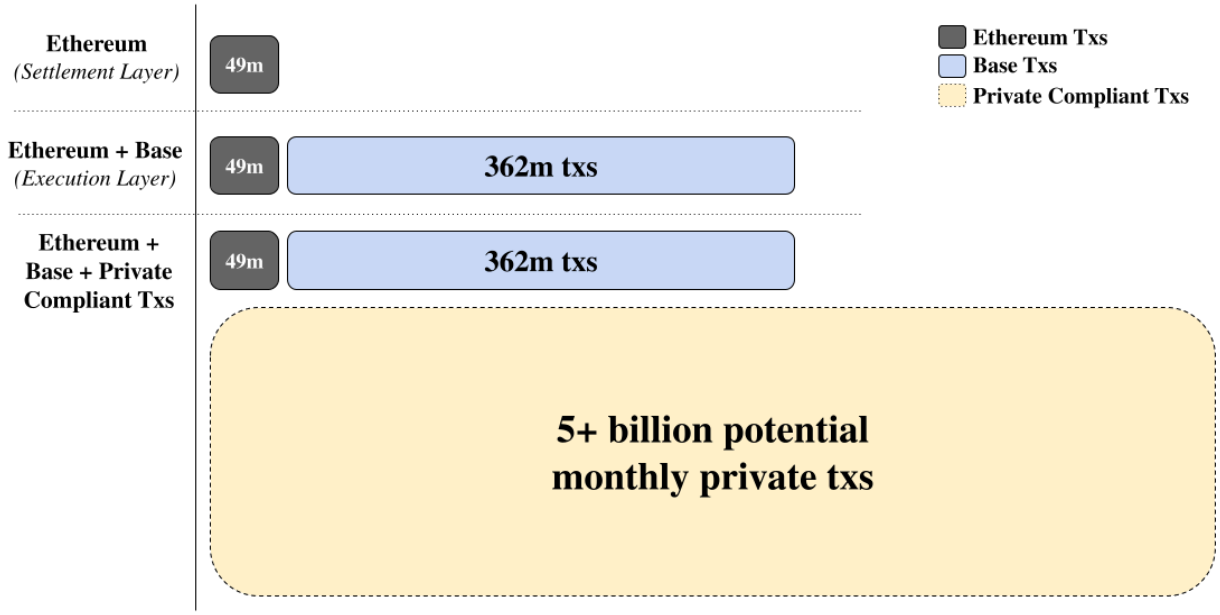

Figure 1: Base has become Ethereum's execution arm, processing millions of monthly transactions - over 7.5x Ethereum's worth of throughput. Yet nearly all of this activity remains public, revealing **latent demand for compliant privacy** that could unlock institutional & enterprise participation at scale.

1.2 From Anonymity to Accountability

Blockchain privacy has evolved from early anonymity networks to the emerging need for accountable confidentiality.

First-generation protocols such as Zcash, Monero, and Horizen's legacy mainchain defined privacy as total anonymity, which was the full concealment of sender, receiver, and transaction flow. While these systems advanced zero-knowledge cryptography, their opacity hindered regulatory acceptance and integration with mainstream finance.

A second wave introduced configurable visibility, aiming to balance privacy with proof of compliance. Projects such as Aleo (private computations with viewing keys) and Aztec (zkRollup with programmable privacy) demonstrated that selective disclosure is possible, but they remain non-EVM ecosystems **disconnected from Ethereum's core liquidity**. Secret Network, based on Cosmos and trusted hardware, follows a similar pattern, innovating outside of Ethereum (Aleo Systems, 2024; Aztec Labs, 2024; Secret Network, 2024). **Privacy research has flourished, yet almost entirely outside the networks where real economic throughput exists.**

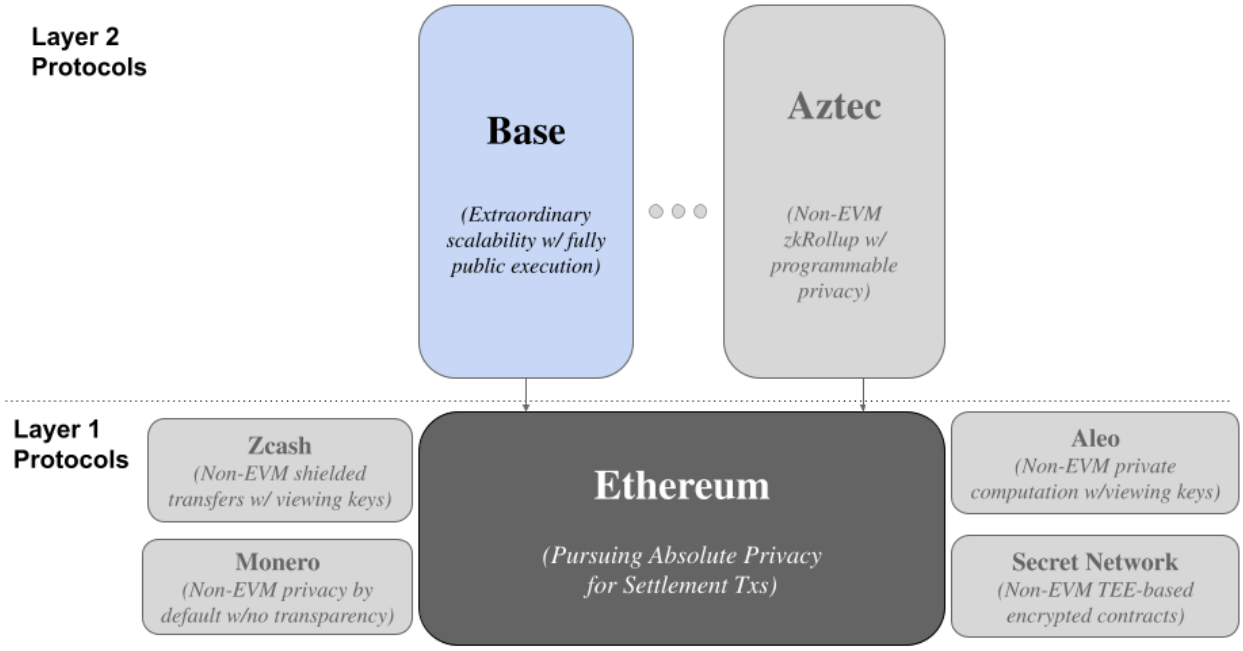

Figure 2: The privacy landscape where innovation hasn't followed liquidity.
Protocol research pursues absolute confidentiality at the settlement layer, while privacy-first chains remain isolated. Meanwhile, liquidity and execution have flourished on Base where it is entirely transparent and without compliant privacy.

Meanwhile, within Ethereum itself, **protocol research continues toward *absolute confidentiality*:** stealth addresses, encrypted mempools, and privacy-preserving account abstraction. These initiatives extend Ethereum's transparency model into encrypted state but intentionally exclude role-based auditability.

At the same time, the privacy problem for enterprises is fundamentally practical rather than ideological. Businesses need privacy not from regulators, but from competitors, security threats, and even internal actors. **They must protect trade secrets, transaction details, and payroll flows** - while still demonstrating regulatory compliance to auditors, supervisors, and tax authorities. Without a framework that can provide both competitive confidentiality and verifiable oversight, adoption among regulated institutions has stalled.

The result is a clear gap: no framework today provides **auditable confidentiality** that aligns with regulatory requirements *and* integrates directly into Ethereum's execution environment. That gap is most visible on Base, now the primary execution hub of the Ethereum ecosystem. Liquidity, user activity, and developer attention have concentrated there, yet every transaction remains fully public. Institutions, enterprises, and fintechs seeking privacy-preserving but compliant transaction rails remain sidelined not because scalability or cost is unsolved, but because **privacy has not followed liquidity**.

The next phase of blockchain privacy will close this divide: **regulatory compliant privacy, a model that fuses cryptographic security with auditability that operates directly where liquidity already lives.** This is the open design space within Base and the broader rollup ecosystem: a privacy layer built for regulated transparency and institutional-grade trust.

1.3 Our Contribution

Horizen extends the capabilities of Base by introducing regulatory compliant, auditable privacy that complements its scalable execution environment and deep liquidity base. Base has achieved what few networks have: mass adoption, robust developer traction, and a concentration of onchain liquidity that anchors the broader Ethereum rollup landscape. Horizen's role is to amplify and extend this success: to bring compliant, privacy-preserving infrastructure directly to where liquidity already flows, accelerating Base's long-term vision for mainstream, institutional-grade adoption.

As one of the first L3 networks deployed on Base, Horizen is designed to complement the Base stack, extending its architecture with privacy and compliance capabilities. Rather than fragmenting liquidity, Horizen moves in tandem with it - aligning its growth, design, and vision with Base to ensure that new capabilities evolve alongside the network's continued expansion.

At its foundation, **the Horizen Protocol** unifies two complementary components that together create a cohesive, compliance-aware privacy architecture centered on Base's liquidity layer:

1. **Horizen Confidential Compute Environment (HCCE)**: A secure hardware-backed execution layer leveraging Trusted Execution Environments (TEEs) to enable attested computation for sensitive logic such as KYC-verified transfers, institutional settlements, and regulated asset issuance.

2. **Horizen Chain**: A privacy-focused blockchain built atop Base, providing encrypted state management and secure coordination between applications, the HCCE, and Base's settlement layer.

Horizen's contribution is to ensure that privacy flows with liquidity. By extending Base's scalable execution layer into a verifiable, compliance-aware privacy framework, the Horizen Protocol advances Ethereum's third transition from transparent scalability to programmable confidentiality.

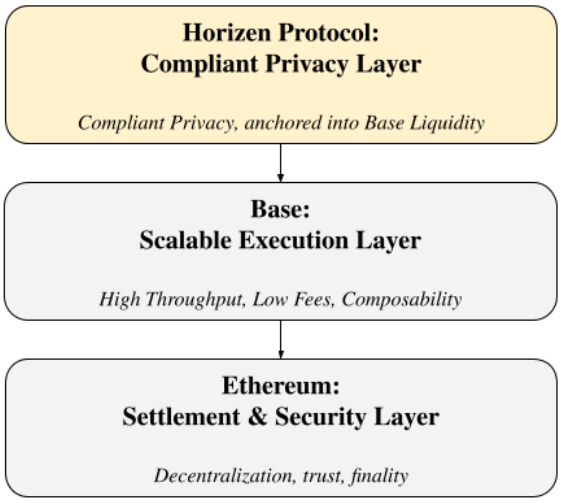

Figure 3: Horizen as a Privacy Layer anchored to Base Liquidity

Horizen builds upon Base's deep liquidity and scalability, adding a compliance-ready privacy layer for confidential, auditable execution. Through its Chain and the Confidential Compute Environment, Horizen expands Base's reach into institutional use cases while preserving its open, composable design.

Horizen complements Base's role as the execution hub of Ethereum, enabling private yet auditable applications to exist within the same liquidity orbit. In doing so, Horizen not only strengthens the Base ecosystem but also delivers the foundational infrastructure for a global, regulatory compliant digital economy - one where privacy and openness coexist by design.

2. Horizen Protocol: Core Architecture

2.1 Architectural Overview

The Horizen Protocol extends Base's execution with attested, confidential computation. **It is built around key design principles: maintain composability with Base's liquidity, preserve verifiability, and embed compliance through attested execution integrity within secure enclaves.** Together, these principles guide every layer of the protocol from

transaction execution and proof generation to cross-domain validation and settlement.

Each of these components plays a distinct yet interdependent role within the Horizen Protocol. The **Horizen Confidential Compute Environment (CCE)** executes sensitive logic within attested, privacy-preserving enclaves, and the **Horizen Chain** coordinates confidential transactions and anchors settlement to Base. The following sections examine each component in greater depth, outlining how together they form a unified system for compliant, auditable privacy within the Base ecosystem.

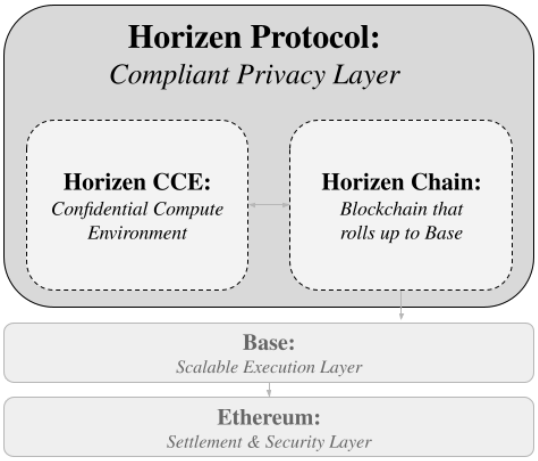

Figure 4: The Horizen Protocol - A Unified Privacy Architecture
The Horizen Protocol consists of two core components - the Horizen Confidential Compute Environment (CCE) and the Horizen Chain - which interoperate to extend Base's execution layer with verifiable and compliant privacy.

2.2 The Horizen Confidential Compute Environment (CCE)

2.2.1 System Overview and Architecture

The Horizen Protocol begins with the Horizen Confidential Compute Environment (CCE), which is a secure execution subsystem that functions as a **confidential coprocessor** to the Horizen Chain. The term coprocessor is used intentionally: just as a hardware coprocessor offloads complex or sensitive operations from a central processor, **the CCE performs confidential and compliance-critical computation on behalf of the Horizen Chain**. This separation allows the system to maintain high performance, transparency, and composability on Base while adding a verifiable layer of secure, attestable computation.

The CCE provides an attested runtime framework where **any application can execute in a privacy-compliant manner.** Instead of requiring privacy-specific design, applications operate within Trusted Execution Environments (TEEs) that guarantee data confidentiality, code integrity, and verifiable auditability. Each enclave produces a signed attestation confirming that the computation was executed by verified hardware running authenticated code under Horizen's compliance policy.

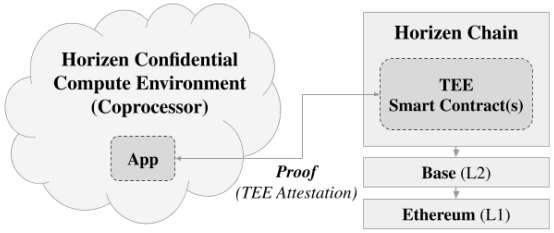

Figure 5: Horizen CCE as a Confidential Coprocessor
The Horizen Confidential Compute Environment (CCE) operates as a secure coprocessor to the Horizen Chain, executing compliance-critical logic inside Trusted Execution Environments while maintaining composability with Base's open execution layer.

At a systems level, the CCE is composed of four interacting components that operate in a tightly coupled feedback loop.

1. **Secure Processor Manager:** Executes code within TEEs, producing attestations that prove the authenticity and integrity of each computation.

2. **On-Chain Smart Contracts:** Governs coordination with the Horizen Chain, validating attestations and linking private execution with transparent settlement.

3. **The Data Layer:** Manages encrypted state and retrieval policies for compliance or audit scenarios.

4. **Authority Service:** Facilitates controlled off-chain access to encrypted reports under dApp-defined policies, ensuring that only authorized entities can retrieve confidential data as permitted.

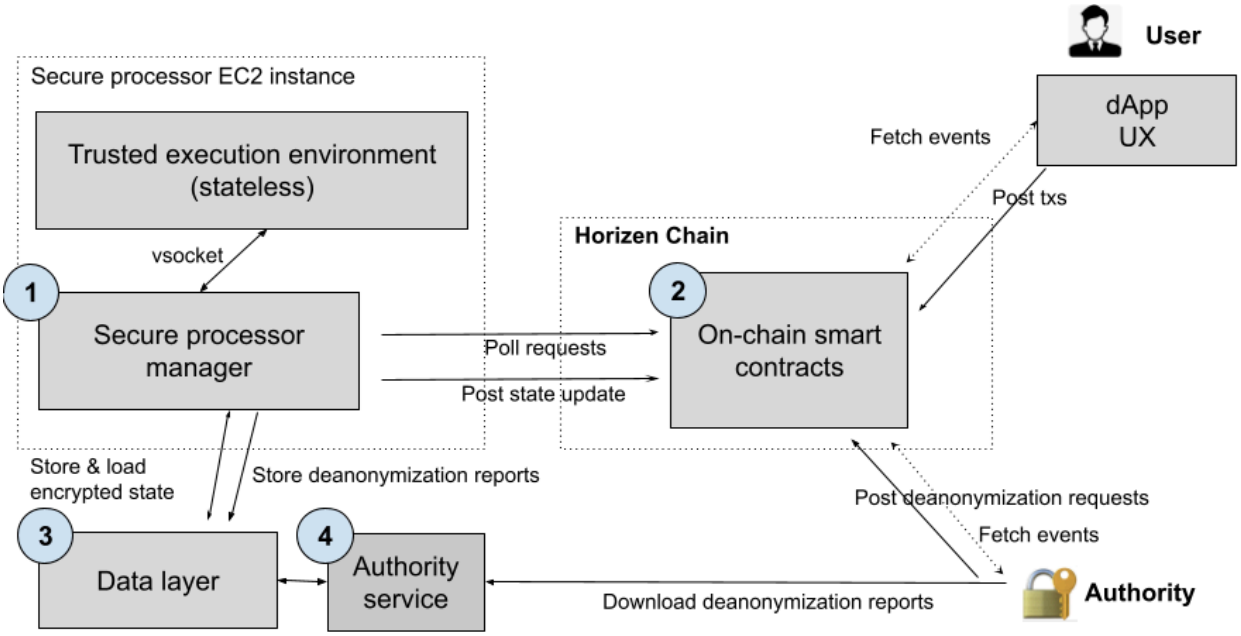

Figure 6: Flexible Compliant-Privacy Framework of the Horizen CCE
Depicts how the Secure Processor Manager, On-Chain Smart Contracts, Data Layer, and Authority Service interact to enable verifiable computation under adaptable compliance policies while preserving confidentiality and composability.

Together, these components form a vertically integrated architecture in which confidential execution, verifiable integrity, and regulatory assurance operate as a single, coherent system. The CCE thus acts as the bridge between private computation and public trust, anchoring Horizen's compliance-aware privacy framework to the liquidity and openness of Base.

2.2.2 Component 1: Secure Processor Manager

The Secure Processor Manager forms the foundational execution layer of the Horizen Confidential Compute Environment (CCE). It serves as the coordinating engine connecting onchain smart contracts, the Trusted Execution Environment (TEE), and the compliance framework-ensuring that every confidential workload proceeds through a verifiable, auditable, and fully encrypted lifecycle.

When a decentralized application (dApp) issues a confidential request through the Horizen Chain, the Secure Processor Manager detects the event emitted by the system's smart contract and polls for new tasks. Upon receipt, it retrieves the dApp's WebAssembly (WASM) module and its encrypted state from the data layer, loads both into the TEE, and initiates execution in an isolated environment.

Throughout this process, encryption is pervasive. Application logic, state, and data payloads remain encrypted at every stage of their lifecycle - during storage, transmission, and verification. The TEE decrypts inputs only within its protected memory space, executes the computation, and re-encrypts all outputs before returning them to the Manager. This ensures that no plaintext data, intermediate state, or execution trace is ever exposed outside the trusted enclave boundary.

Inside the TEE, the dApp executes according to its declared compliance level. **Any authorization rules are strictly optional and implemented only when explicitly defined by the developer.** For example, the dApp which transactions may later be audited or de-anonymized by authorized entities. Upon completion, the TEE produces an updated encrypted state, encrypted events or withdrawals, and a TEE-signed attestation confirming that the computation was performed on verified hardware using authenticated code.

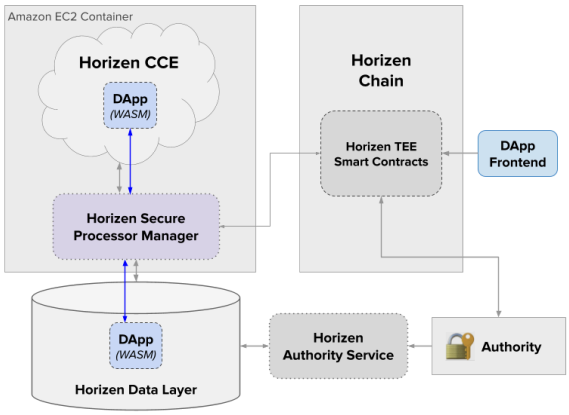

Figure 7: The role of Secure Processor Manager within the CCE

Depicts how the Secure Processor Manager orchestrates dApp-defined confidential computation within the TEE, loading encrypted logic and state, executing under application-specific compliance rules, and committing attested, encrypted results to the Horizen Chain.

The Secure Processor Manager then commits this attested output to the onchain contract, anchoring private computation to public settlement. **Applications are loaded and unloaded ephemerally, ensuring each computation starts from a clean, attested instance.** This ephemeral model, combined with universal encryption, guarantees that no residual plaintext data or code persists across executions.

Through this event-driven and stateless architecture, the Secure Processor Manager enables decentralized applications to operate privately yet transparently - binding compliant confidentiality to the liquidity and openness of Base while maintaining verifiability at every layer of the Horizen Protocol.

2.2.3 Component 2: On-Chain Smart Contracts

The onchain smart contracts form the coordination and verification layer that links the Horizen Confidential Compute Environment (CCE) to the public settlement of the Horizen Chain. They validate attestations, manage encrypted state references, and enforce policy context - all without exposing private data or application logic.

This contract layer is composed of three primary modules:

1. **ProcessorEndpoint**: Coordinates confidential computation requests and responses between decentralized applications and the CCE.

2. **TeeAuthenticator**: Checks the correctness of the payload produced by the TEE.

3. **AuthorityRegistry**: Records the entities allowed to request de-anonymized data.

Together, these modules establish the verifiable interface that connects encrypted off-chain execution to transparent onchain settlement.

The ProcessorEndpoint serves as the operational hub. It queues incoming confidential workloads from decentralized applications, tracks their lifecycle, and records the resulting attestations generated by the Secure Processor Manager. Each attestation (representing a verified computation within the TEE) is validated for authenticity and immutably committed onchain. The contract maintains pointers to the encrypted state stored in the Data Layer, ensuring that while attestations are public, all data and logic remain fully encrypted.

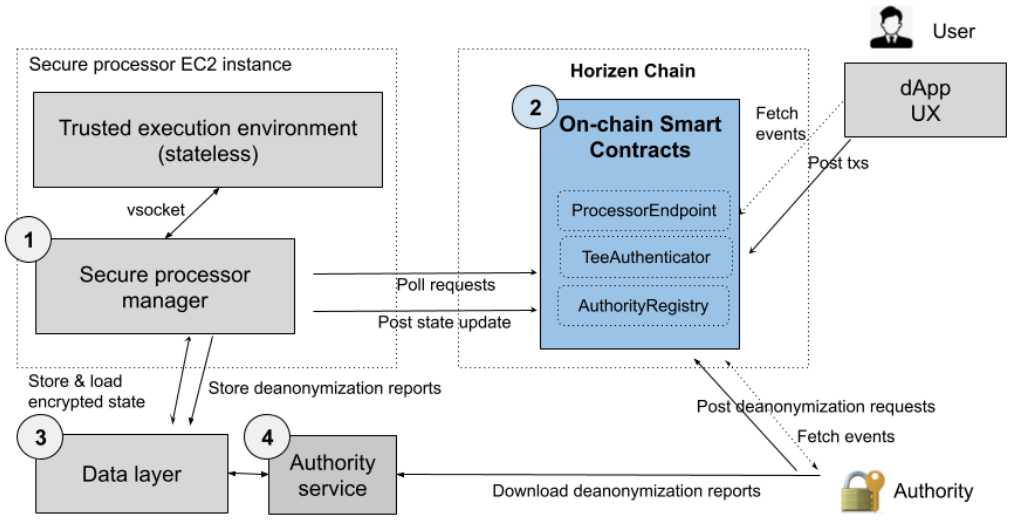

Figure 8: On-Chain Smart Contracts for Encrypted, Compliant Workflows
Depicts how Horizen's onchain contracts (ProcessorEndpoint, TeeAuthenticator, and AuthorityRegistry) coordinate encrypted execution flows, validate attestations, and maintain compliance metadata, enabling verifiable computation and settlement without exposing underlying data or logic.

The TeeAuthenticator verifies the correctness of the TEE attestation payload. It executes an onchain verification of the payload signature coming from the TEE, providing the guarantee the data has been processed by the expected software in the expected secure enclave, and the result has not been tampered by the processor manager.

The AuthorityRegistry is an entrypoint for checking the entities allowed to request data deanonymization. It provides a default mechanism to identify the authorities (implemented by an admin-managed whitelist), but allows every application to define a more custom logic via a specialized smart contract.

By design, Horizen's onchain smart contracts transform the CCE into an auditable subsystem of Base's broader execution environment. **They uphold composability and transparency while ensuring that privacy and compliance remain verifiable through cryptographic proof rather than disclosure.**

2.2.4 Component 3: Data Layer

The **Data Layer** provides the encrypted persistence backbone of the **Horizen CCE**. It offers a secure API for storing, retrieving, and auditing all data produced by decentralized applications (dApps), ensuring that every element of a computation – from bytecode to state and compliance records – remains encrypted at rest, in transit, and during retrieval.

Each dApp operates as a self-contained entity within this framework, maintaining its **own encrypted internal state** and data model. The Data Layer allows every dApp to define how its private state is organized – whether as a ledger, liquidity pool, order book, or another domain-specific structure. These data structures are coupled to the dApp's WASM logic, which enforces transaction rules, compliance controls, and workflow constraints inside the TEE.

Three principal kinds of data are managed through the Data Layer API:

- **WASM application bytecode**, representing the executable logic of each dApp.

- **Application state**, encrypted with the TEE key, preserving confidentiality so that only attested execution environments can decrypt or update it.

- **Deanonymization reports**, encrypted with an authority key, enabling authorized oversight under defined compliance contexts.

After every confidential execution, the TEE commits the updated **encrypted state root** to the Horizen Chain, anchoring the computation to a verifiable public record. The corresponding full encrypted state is stored in the Data Layer for **durability, recovery, and compliance audits**. Each new state version links cryptographically to the previous one, forming an immutable and verifiable history of encrypted state transitions without revealing underlying data. Additionally, the Data Layer is structured to allow flexibility in adopting decentralized data-availability options to ensure resilience and long-term verifiability.

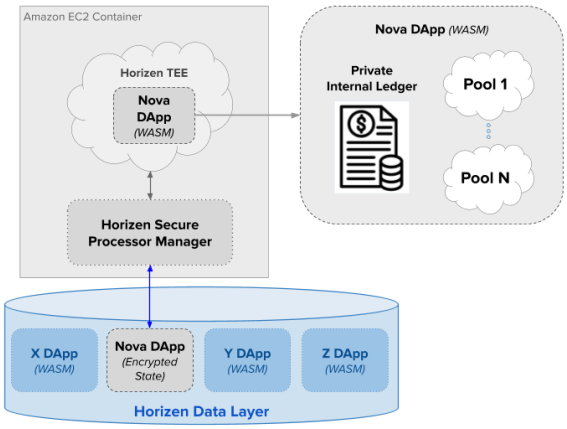

Figure 9: Data Layer for Encrypted State & Compliance Persistence

Depicts how each dApp defines and manages its own encrypted data structures, WASM logic, and compliance artifacts, with every state update committed onchain and the full encrypted state persisted for durability and auditability.

This dApp-centric design ensures that encryption is pervasive and persistent - no plaintext bytecode, key, or report ever exists outside attested environments. By coupling private data ownership with verifiable auditability, the Data Layer allows decentralized applications to achieve true compliant privacy while remaining composable with the public settlement and liquidity of Base.

2.2.5 Component 4: Authority Service

The Authority Service provides the oversight and auditability framework that enables privacy to coexist with regulatory and organizational accountability. It allows authorized entities to request, verify, and decrypt audit artifacts through controlled, onchain governance - ensuring that transparency is verifiable, scoped, and cryptographically enforced.

At its core, the Authority Service operates under an **authority-based model**, where each dApp defines its own compliance structure and associated oversight entities. These **authority entities** (such as custodians, compliance officers, or designated auditors) are registered onchain and validated through authenticated public keys or decentralized identifiers (DIDs). This establishes a verifiable link between a dApp's internal policy and its external accountability framework.

This model differs from traditional viewing-key systems, which delegate disclosure to individual users and often lack reliable audit trails. In Horizen's design, disclosure is mediated through cryptographic attestations and onchain events, ensuring that access occurs only within an auditable and verifiable process defined by the dApp's compliance policy.

When an authorized entity initiates a deanonymization request, the Authority Service coordinates the process through onchain smart contracts. It validates the requester's credentials and verifies that the request conforms to the dApp's registered policy parameters. Once confirmed, the system triggers an invocation of the TEE. Inside the enclave, the Secure Processor Manager generates a **deanonymization report** (encrypted with the authority's public key) containing only the approved

subset of information, such as transaction metadata, balance proofs, or identity attestations.

Each deanonymization event is immutably recorded onchain, providing a cryptographic record of access without disclosing the contents of the report. This creates a two-fold structure of accountability:

1. **On-chain transparency**, through visible records of every access request and attestation.

2. **Cryptographic containment**, through key-based encryption that limits data visibility strictly to approved authorities.

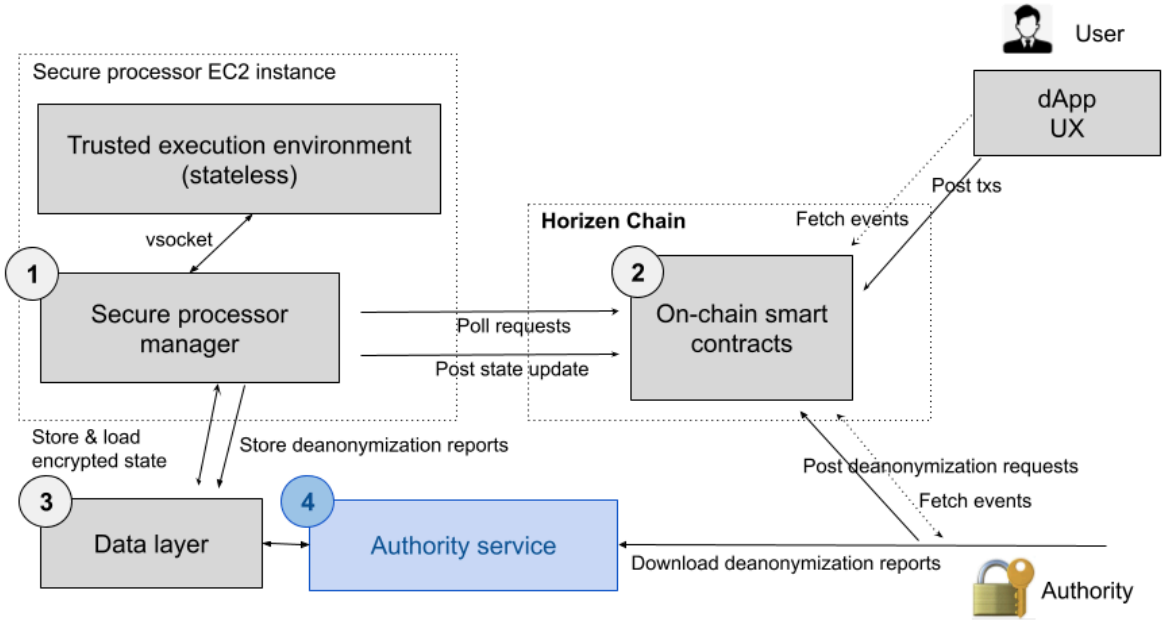

Figure 10: Authority Service for Encrypted Oversight & Auditability
Depicts how the Authority Service authenticates registered authorities, retrieves encrypted deanonymization reports, and enables verified access under onchain accountability in accordance with dApp-defined compliance rules.

The Authority Service is tightly integrated with the **Data Layer** and **AuthorityRegistry**, enabling controlled retrieval of encrypted records for audits and compliance verification. Every request, authorization, and output remains encrypted end-to-end, preserving the confidentiality of the underlying data while allowing external validation of compliance activity.

Through this architecture, the Authority Service establishes a verifiable model of **compliant privacy**, where decentralized applications can satisfy oversight and regulatory expectations without sacrificing confidentiality. It bridges cryptographic integrity with institutional accountability, allowing Horizen to support enterprise, financial, and public-sector applications that require both privacy and verifiability.

2.2.6 Redundancy Considerations

As with any form of hardware-backed execution environment, TEEs may encounter faults, deprecations, or newly discovered vulnerabilities over time. The Horizen Protocol is designed with this reality in mind: **the system supports enclave rollover and re-attestation, allowing faulty or outdated TEEs to be safely replaced without disrupting dApp state or execution guarantees.**

Looking forward, the protocol treats TEE redundancy as an ongoing design consideration, prioritizing mechanisms that allow execution to continue even when individual enclaves must be rotated out for security or reliability reasons.

2.3 Horizen Chain

2.3.1 Chain Architecture and Base Anchoring

The Horizen Chain forms the execution and settlement backbone of the Horizen Protocol. It is purpose-built to extend Base's scalability and liquidity into a compliant-privacy domain by combining three key architectural elements: anchoring to Base's native data-availability layer, fast omnichain bridging through Stargate V2 (LayerZero), and confidential execution through the Horizen Confidential Compute Environment (HCCE). Together, these components allow Horizen to maintain interoperability with Base's ecosystem while enabling verifiable, compliance-ready privacy.

1) **Base-Anchored Rollup**
   Horizen operates as an OP Stack L3 rollup that publishes its transaction data and state commitments directly to Base's native DA layer. This anchoring model allows Horizen to inherit Base's scalability, composability, and sequencing infrastructure while remaining economically aligned with Ethereum. By finalizing all data and proofs on Base, Horizen inherits Ethereum's security and finality guarantees implicitly through Base, creating a unified trust model from confidential execution to public settlement.

2) **Fast Bridging via Stargate V2 (LayerZero)**
   Interoperability and liquidity between Horizen and Base are facilitated by Stargate V2, LayerZero's cross-chain routing primitive designed for unified liquidity across networks (LayerZero Labs, 2025). At launch, **native ETH** serves as the first supported asset with shared liquidity pools between Horizen and Base, enabling transfers that settle within seconds and achieve guaranteed finality without wrapped or re-minted tokens. Stablecoins such as **USDC.e** are bridged through Hydra's Omnichain Fungible Token (OFT) framework (HydraDX, 2025). Support for additional assets (such as WBTC, cbBTC, and cbETH) is planned through a combination of custom OFT deployments or dedicated Stargate V2 pools as the ecosystem matures. **This bridging framework ensures that privacy-oriented dApps on Horizen can access Base's liquidity directly** while maintaining seamless composability within the broader Ethereum and Superchain environment.

3) **Connection to the Horizen Confidential Compute Environment (HCCE)**
   Each application deployed on the Horizen Chain can connect natively to the HCCE, where its logic executes inside attested TEEs. The chain provides standardized runtime APIs for dApps to offload private computation, receive encrypted results, and anchor attested state roots and compliance metadata onchain. This linkage ensures every confidential operation executed within the HCCE is transparently verifiable on Base through Horizen's settlement process, preserving both privacy and auditability.

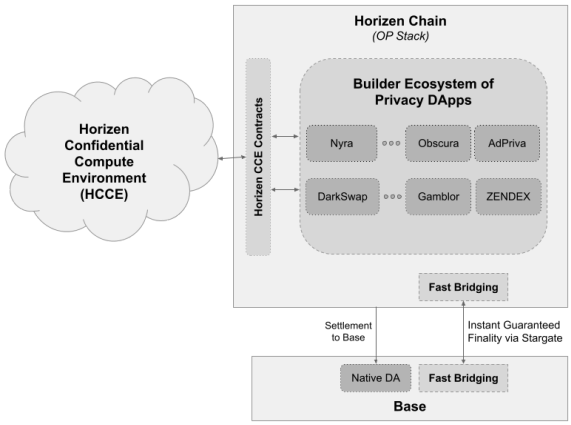

Figure 11: Horizen Chain and Base Anchoring
Depicts the three foundational elements of the Horizen Chain: Base-anchored rollup settlement, fast bridging via Stargate V2, and secure connection to the HCCE for confidential execution and policy-aware computation.

2.3.2 Ecosystem of Privacy DApps

The Thrive Builder Funding Program is the **primary growth engine of the Horizen Chain**, established in partnership between Horizen and Thrive Protocol to fund privacy-first builders across the Base ecosystem. Season 1 of the program allocates 200,000 ZEN in funding for approximately 25 to 50 high-impact projects, with average grants of $50,000 - $100,000 per project. Funding is milestone-based and results-driven, tracking total value locked in ZEN, transaction volume, and active wallets as key metrics of network growth and impact (Thrive Protocol, 2025). The program supports projects that advance privacy as core infrastructure for decentralized applications. Approximately **40%** of funding targets privacy-centric DeFi protocols (e.g., private DEXs, confidential lending, hidden order books), **30%** supports verified AI and machine-learning use cases (such as privacy-preserving training and ZK model verification), and **30%** is directed toward gaming and governance systems (including private voting and ZK-based reputation).

All applications deployed on the Horizen Chain have the ability to access **fast omnichain bridging via Stargate V2** and the **Horizen Confidential Compute Environment (HCCE)** if desired, enabling rapid liquidity movement and confidential execution within a unified compliance framework. By combining Horizen's privacy-focused chain architecture with Thrive's GDP-layer funding model, the program establishes a merit-based ecosystem that rewards measurable adoption and advances the future of compliant privacy on Base. For economic design and sustainability details, see the **Horizen Tokenomics Whitepaper** (Horizen Labs, 2025).

2.3.3 Near-Term Roadmap

The Horizen Chain is designed as a continuously evolving privacy infrastructure that advances in parallel with Base and the broader Superchain ecosystem. Each phase strengthens the protocol's compliance, verifiability, and interoperability while preserving alignment with Base's liquidity and the Horizen Confidential Compute Environment (HCCE).

1. **Base Anchoring & Liquidity Alignment**

   Horizen Chain anchors to Base's native data-availability layer, inheriting its scalability, security, and settlement guarantees. This phase also establishes fast cross-chain bridging through Stargate V2, enabling shared liquidity between Horizen and Base and forming the foundation for subsequent privacy-focused upgrades.

2. **Phase 2: Confidential Execution & Compliance Toolkit**

   Building on this foundation, Phase 2 introduces confidential execution via the HCCE, supported by a built-in compliance and authorization framework. It establishes a compliance toolbox for KYC, accreditation, and privacy-preserving identity (DID / zkID), allowing applications to meet regulatory requirements without sacrificing privacy or composability.

3. **Phase 3: Validity Proofs & Accelerated Finality**

   The final phase integrates validity-proof frameworks such as OP Succinct and Risc Zero Kailua to replace the traditional optimistic challenge window with cryptographic verification, reducing settlement times from days to minutes. This advancement delivers fast, verifiable withdrawals and cross-chain settlement between Horizen and Base, completing the progression toward fully verifiable privacy infrastructure.

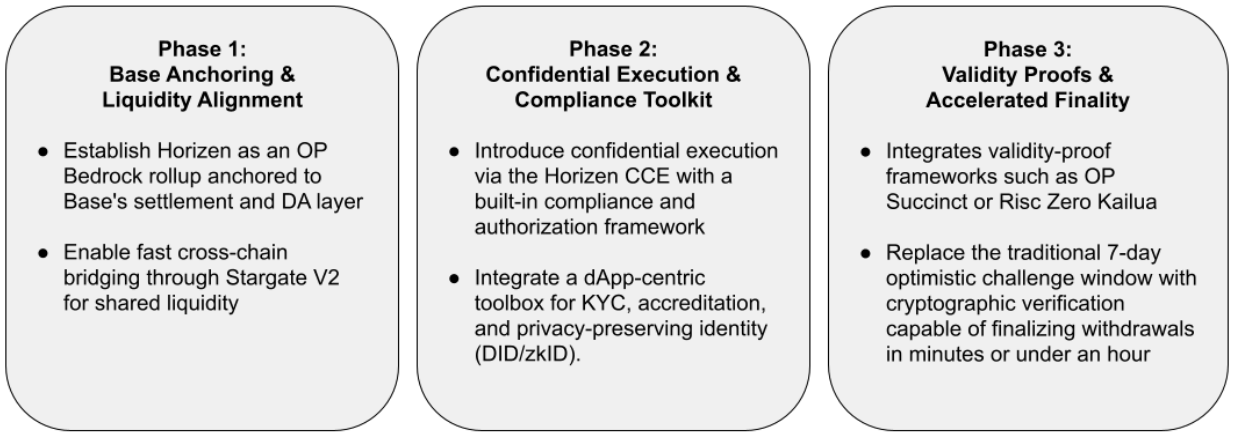

Figure 12: Horizen Chain Near-Term Roadmap

Shows the three developmental phases of the Horizen Chain: Base anchoring, chain-level compliance, & validity-proof verification - illustrating its progressive evolution toward faster and more verifiable privacy execution.

Together, these phases outline a clear trajectory from anchored compliant execution to cryptographically verified confidentiality, ensuring that Horizen evolves as a foundational, Base-aligned privacy infrastructure.

3. Applied Research at the Privacy Frontier

3.1 Privacy as a Progressive Continuum

Horizen also views compliant privacy as a **progressive continuum**, not a static endpoint. The current protocol represents a practical first phase, built on TEEs and ZK verification. Future iterations are designed to evolve alongside emerging technologies such as **Fully Homomorphic Encryption (FHE)** and next-generation **ZK proof systems**, allowing the Horizen Protocol to adapt as Base and the broader Superchain ecosystem advance toward deeper programmable privacy. Horizen's **Privacy Development Roadmap** is divided into four stages, each of them integrating progressively more advanced technologies in order to achieve more and more robust privacy applications.

3.2 Stage 0: Near-Term

Our choice to initially build on TEEs is a deliberate and strategic decision rooted in pragmatism. While purely cryptographic solutions like general-purpose Zero-Knowledge Proofs (ZK) and FHE hold immense promise for the future of onchain privacy, they are not yet mature enough for widespread, production-grade deployment. ZK systems currently face significant challenges with high proving times, circuit complexity, and poor developer ergonomics, while FHE remains orders of magnitude too slow for most practical applications.

In contrast, TEEs offer a solution that is mature, performant, and deployable *today*. The key advantages that make TEEs the ideal foundation for Horizen's compliant privacy layer include:

- **Production Readiness:** TEE technology is a mature field, with hardware-backed solutions widely deployed in data centers and cloud environments globally.
- **Near-Native Performance:** Computation within a TEE occurs at speeds close to native execution, avoiding the latency and computational overhead associated with current ZK and FHE systems.

- **Developer-First Approach:** The Horizen Confidential Compute Environment is designed to support mainstream development workflows. It accommodates widely used programming languages like Go and Rust (and any language able to generate WebAssembly), allowing developers to leverage existing tools, libraries, and expertise. This dramatically reduces the barrier to entry and accelerates the development of privacy-preserving applications, as builders are not required to learn entirely new cryptographic paradigms or complex circuit design languages.

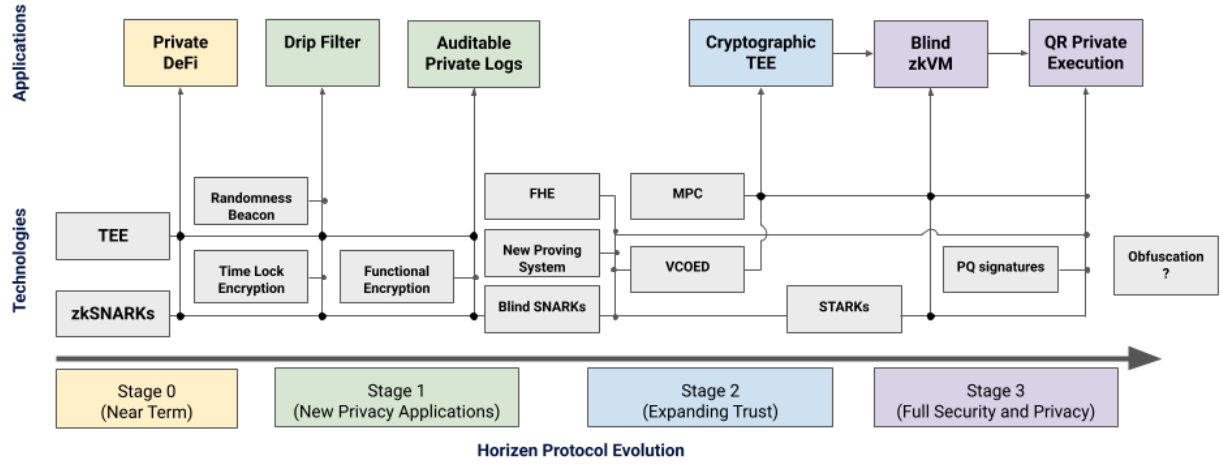

Figure 13: Horizen Protocol: A Progressive Research Roadmap

Outlines the four-stage pathway guiding the Horizen Protocol's applied-research agenda, bridging deployed confidentiality with forward-looking work in scalable verification and decentralized compliance frameworks.

The Horizen Chain establishes the groundwork for a new generation of privacy-enabled applications built on its foundational architecture. These include **DarkSwap**, the first bot-resistant decentralized finance protocol providing private order execution before settlement; **Gamblor**, a provably fair gaming and betting platform; **ZENDEX**, a ZK-powered decentralized exchange for private trading; **Nyra**, a privacy-focused perpetuals exchange leveraging secure execution environments; **AdPriva**, a user-owned advertising network replacing cookies with cryptographic proofs; and **Obscura**, a verifiable reputation layer for DeFi and social trading. Collectively, these applications illustrate how Horizen's Base-anchored infrastructure is positioned to support scalable privacy innovation - from private trading and gaming to privacy-preserving advertising and identity systems.

3.3 Stage 1: New Privacy Applications

Stage 1 in the research and development of the Horizen Privacy Roadmap is about including novel privacy applications that are relatively low-hanging fruits in terms of implementation once the research stage is completed.

For example, we are looking at the design of what we call **Drip Filter**. **This smart contract-based protocol serves to break sender-receiver linkability by obscuring transactions within network traffic.** The drip filter takes a deposit transaction from the sender that includes a timing parameter in the metadata and breaks it (randomly and unpredictably) into smaller transactions, each encrypted under time-lock encryption. These time-lock encrypted transactions are stored on a public ledger along with dummy transactions to hide the connection between a deposit and the subsequent ciphertexts. The ciphertexts can only be decrypted

after the given time, by any party, including the receiver, to obtain presigned withdrawal transactions. **The analogy is: pouring a batch of hot water into a drip filter (the incoming transaction) and then the coffee is released (sent to the receiver) as smaller "drops" at irregular, unpredictable intervals.**

The filter further provides the sender with a transferable zero-knowledge receipt: a ZKP that the transactions have been committed and cannot be reverted, that the sum of these transactions is equal to the original deposit, that the transactions send funds to the intended receiver, and that all ciphertexts will be decryptable within the time chosen by the sender. This "cryptographic receipt" can be used as a transferable proof that the transaction is on the way.

For achieving privacy, the sender-receiver link is obscured through many users passing transactions through the filter. For example, if both Alice and Bob pay Charlie through our filter, the withdrawal transactions from Alice's deposit and Bob's deposit are indistinguishable. **This protocol is of independent interest as it makes minimal assumptions about the underlying chain**: we make no assumptions of privacy or any specific transaction structure aside from the existence of metadata in transactions. Our protocol uses TEEs, but this can also be replaced, in principle, by a committee of nodes. Additionally, randomness beacons and time-lock encryption are used.

Drip filters also mitigate front-running, as large transactions are often a target of front-running attacks, without modifying the logic of the underlying chain. Further, drip filters overcome the fixed deposit limitation of tools like TornadoCash, implement futures contracts, and demonstrate an interesting use-case for time-lock encryption.

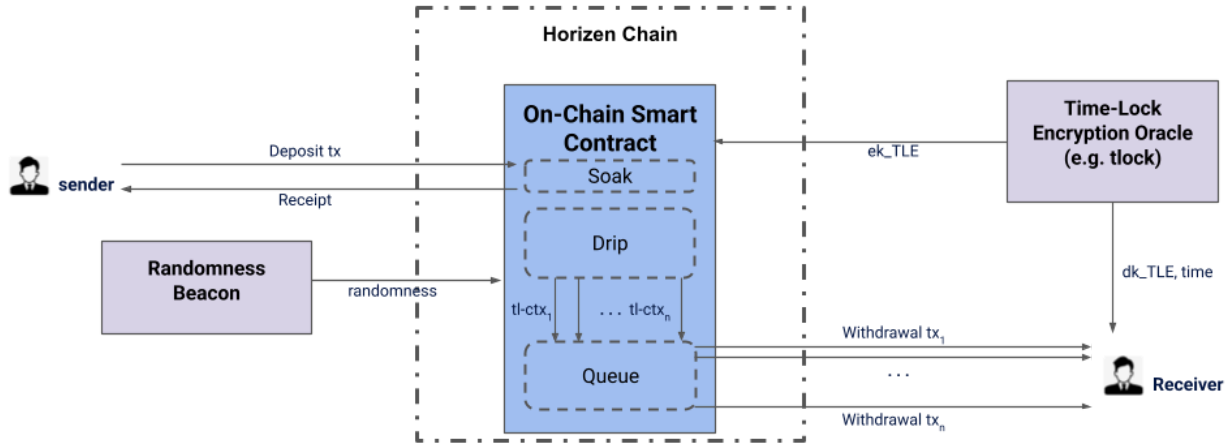

Figure 14: Horizen Drip Filter - Timed Private Transfers

Named for its gradual, filtered release of value, the Drip Filter divides a deposit into randomized micro-transfers emitted over time. This "dripping" mechanism conceals behavioral patterns & transaction linkages without altering base-layer logic, achieving privacy through controlled timing rather than anonymity sets.

Another application we are researching with our current technology stack is some form of Auditable Private Logs using Functional Encryption (FE). FE is similar to FHE, with the difference that the output of the evaluation of the circuit is not encrypted, but rather in cleartext.This is useful if, given a certain ciphertext, we want to give the possibility of computing some specific function on the underlying plaintext, but nothing else. For example, in the context of **Private Inference for AI**, we might look at techniques that allow a user to query a private AI model using privacy-preserving technology in such a way that 1) nobody, even the

provider of the model, can read the user's queries; and 2) at the same time, anyone can evaluate a function on those queries, which reveal whether, e.g., the user's query is "too close" (in term of some multidimensional metric) to a set of "forbidden queries" (the model's guardrails), thereby offering a very fine-grained level of selective compliance.

3.4 Stage 2: Expanding Trust

Horizen's current architecture, centered on TEEs, is a pragmatic and deliberate choice to deliver a functional, high-performance confidential computing environment today. However, our long-term vision for privacy is rooted in pure, verifiable cryptographic guarantees, moving beyond reliance on trusted hardware. The system is designed with modularity and extensibility in mind, serving as a bridge between the immediate needs of the market and the long-term vision of a fully trustless future. Our research and development roadmap is focused on integrating a series of cutting-edge cryptographic primitives to progressively enhance decentralization, security, and confidentiality.

When looking at verifiable computation, the integration of **Blind Zero-Knowledge Proofs** and **Fully Homomorphic Encryption** would allow us to move beyond TEE attestations to certify correctness of execution by building a powerful primitive known as **Verifiable Computation Over Encrypted Data (VCOED)**, which in turn allows to perform a private computation over private data with assurance that the computation has been performed correctly (a sort of **"cryptographic TEE"**). Unlike the stronger but less performant **Verifiable Fully Homomorphic Encryption (VFHE)**, VCOED allows for a certain degree of adversarial malleability on the ciphertext, as long as the underlying plaintext remains private and unaltered. This feature can actually be seen as an advantage in certain privacy applications, such as the possibility of re-randomizing signatures and ciphertexts without impacting security. This would allow the Horizen Protocol to disconnect completely from the vendor-provided hardware assurance of the TEE, aiming for a fully transparent and more robust replacement.

3.4 Stage 3: Full Security and Privacy

When looking at the future of privacy and security, Horizen's goal is to meet the strongest requirements that are demanded from market dynamics and industry regulations. This includes **Quantum Security** and **Fully Private On-Chain Computation**.

Unlike other ZK systems such as SNARKs, **STARKs (Scalable Transparent Arguments of Knowledge)** are natively quantum-resistant and do not require a trusted setup, aligning perfectly with our goal of a truly trustless system. This will allow the protocol to cryptographically prove the integrity of off-chain computations without relying on the security assumptions of a hardware vendor.

To mitigate single points of failure and enhance operational security, we look at advanced **Multi-Party Computation (MPC)** protocols. A primary use case is the introduction of **hierarchical threshold signatures** for managing critical protocol functions and user assets. This would decentralize control, requiring a quorum of independent parties to authorize actions, thus providing robust safeguards against collusion and compromise.

Our ultimate goal is to enable arbitrary, privacy-preserving smart contracts in a fully trustless and post-quantum secure manner, enabling applications such as a **scalable and fast zkEVM**, a **plug-in compliance layer for arbitrary privacy applications**, and **verifiable and private computation for AI training, inference, and certification**. By pursuing this ambitious roadmap, Horizen aims to evolve from a pragmatic, TEE-based privacy layer into the foundational infrastructure for a truly secure, verifiable, and future-proof digital economy.

4. Use Cases and Market Opportunities

Horizen's architecture is designed to unlock a wide range of high-value applications that are currently impractical on transparent public blockchains. By providing a platform for compliant privacy, Horizen translates its technical capabilities into tangible business value across several key markets.

4.1 Confidential Stablecoins and Encrypted Payments

The HCCE provides the ideal infrastructure for the next generation of stablecoins and payment systems. **Issuers can deploy stablecoin logic within a secure enclave, enabling features such as encrypted balances and private peer-to-peer transfers.** This allows individuals and businesses to transact without broadcasting their financial activities to the public. Crucially, this privacy is not absolute. The system supports selective auditability through the use of programmable privacy, allowing users to prove their transaction history to authorized parties like regulators or tax authorities without compromising their day-to-day confidentiality. This combination of privacy and control creates a foundation for stablecoins to be safely used in sensitive applications like B2B settlement, payroll, and global commerce.

4.2 Confidential DeFi

Horizen extends privacy into decentralized finance through the Horizen CCE, enabling confidential trading, lending, and liquidity operations that maintain composability with the Base ecosystem. Unlike solutions that protect order flow only before settlement (such as Flashbots), Horizen preserves confidentiality both before and after execution. While Flashbots shield transactions from front-running and MEV prior to inclusion, all activity becomes publicly visible once finalized onchain. **Horizen's design ensures that pricing strategies, positions, and counterparties remain encrypted even after settlement**, allowing traders and protocols to retain competitive privacy without compromising auditability or regulatory compliance.

Fully cryptographic systems such as those based on ZK proofs or FHE remain too slow for high-frequency or real-time market applications. Horizen overcomes these performance barriers by supporting low-latency confidential execution, enabling strategies that require rapid price discovery and responsive order management. This balance between speed and confidentiality makes privacy-preserving finance not only secure but also practical for modern markets. Together, **these capabilities define a new class of confidential financial infrastructure** - one that unites persistent privacy with verifiable transparency, delivering institutional-grade performance within the Base ecosystem.

4.3 Verifiable AI and Autonomous Agents

The Horizen Protocol provides a foundation for running verifiable, privacy-preserving AI models and autonomous onchain agents that operate under compliance-aware rules. Applications can deploy AI-driven logic for tasks such as credit scoring, portfolio management, fraud detection, or automated governance, while maintaining confidentiality over proprietary data, model parameters, and decision processes. **Outputs are verifiable and auditable**, ensuring accountability without exposing the underlying algorithms or sensitive inputs.

Existing ZK and FHE frameworks face significant performance limitations that make such AI use cases impractical today. **Running model inference or agent reasoning within ZK or FHE systems introduces latency and computational overheads** several orders of magnitude higher than acceptable for real-time or high-throughput environments. Horizen addresses this gap by enabling verifiable AI execution at native speed, preserving data privacy and model integrity while remaining performant enough for continuous, autonomous operation. This capability unlocks a new generation of intelligent, compliant, and confidential applications - where agents can act independently on encrypted data, generate verifiable outputs, and interact seamlessly with both DeFi protocols and Base's broader ecosystem.

5. ZEN Utility

ZEN anchors the economic and governance logic of the Horizen ecosystem. While the Horizen Protocol leverages ETH, USDC, and ZEN, all three assets feed into a single circular value system that links protocol activity to token demand. This mechanism is transparent, market-based, and **modeled on frameworks like Optimism's OP token**, in order to coordinate governance, align incentives, and capture ecosystem value.

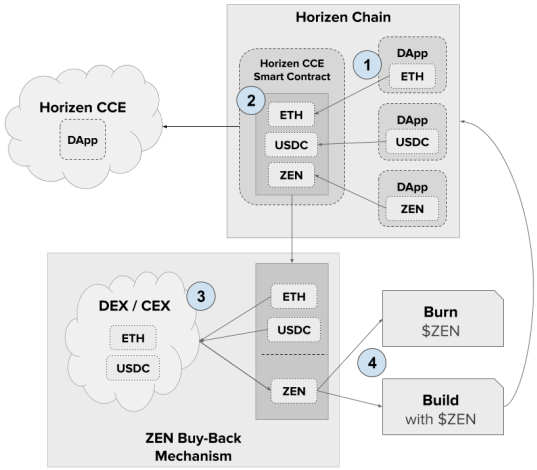

Figure 14: Horizen Drip Filter - Timed Private Transfers

Named for its gradual, filtered release of value, the Drip Filter divides a deposit into randomized micro-transfers emitted over time. This "dripping" mechanism conceals behavioral patterns & transaction linkages without altering base-layer logic, achieving privacy through controlled timing rather than anonymity sets.

5.1 Flow of ZEN Utility

1. **Utility Through Execution**
   DApps across the Horizen Chain can use **ETH, USDC, or ZEN** to pay for execution, compute operations, or state updates within the Horizen CCE.

2. **Fee Collection and Vaulting**
   A portion of the payments received from these executions are collected into a smart-contract vault, aggregating value generated across both the Horizen Chain and CCE.

3. **Buyback Mechanism**
   At defined intervals, a portion of vault balances (ETH and USDC) is used to perform **open-market buybacks of ZEN** through decentralized or centralized exchanges. This establishes a direct feedback loop, where greater application usage translates into greater token demand.

4. **Burn or Build Cycle**
   The ZEN acquired through buybacks is either:
   - **Burned**, permanently reducing circulating supply, or
   - **Reinvested**, funding ecosystem development, research, and new dApp incentives through programs such as **Thrive**.

This process transforms protocol activity into a self-reinforcing value engine: **usage → revenue → buyback → growth**, without relying on inflationary emissions. For further details on buyback parameters, treasury operations, and token flows, refer to the **Horizen Tokenomics Whitepaper (Horizen Labs Research, 2025)**.

5.2 Comparative Utility and Regulatory Position

Like Optimism's OP token, ZEN is not used for network security nor as a mandatory gas asset. It functions instead as a governance and value-capture token, enabling coordinated decision-making and treasury-backed sustainability. ZEN remains a transparent ERC-20 token on Base, ensuring full composability, auditability, and regulatory clarity.

6. Conclusions: The Foundation for a Privacy Layer on Base

The Horizen Protocol establishes a new privacy foundation for the Base and Ethereum ecosystems - one that harmonizes confidentiality with verifiability, performance, and regulatory readiness. **Built around the Horizen Chain and the Horizen Confidential Compute Environment (HCCE), the protocol extends Base's scalable execution with attested computation, encrypted data management, and policy-aware design.** This architecture enables developers to build applications that operate privately

by default while remaining composable, auditable, and interoperable with public networks.

Through progressive research and deployment, **Horizen advances a continuum from pragmatic confidentiality to cryptographic verifiability.** Each stage - from today's Base-anchored execution to future phases integrating validity proofs and programmable privacy - contributes to a broader goal: making privacy not a niche feature, but a foundational property of decentralized systems.

In this model, ZEN anchors the protocol's economic and governance logic, coordinating compute access, network incentives, and ecosystem alignment. **Together, these components define Horizen's contribution to the next generation of privacy infrastructure** - one where compliant, verifiable privacy becomes a catalyst for institutional adoption and scalable onchain innovation.

References

- Aleo Systems. (2024). *Aleo Developer Documentation.* Retrieved from https://developer.aleo.org
- Arapinis M., Lamprou N., Zacharias T. Astrolabous: *A universally composable time-lock encryption scheme.* ASIACRYPT 2021.
- Arnon G., Chiesa A., Fenzi G., Yogev E. *WHIR: Reed-Solomon proximity testing with super-fast verification.* EUROCRYPT 2025.
- Aztec Labs. (2024). *Programmable Privacy and zkRollup Architecture.* Retrieved from https://docs.aztec.network
- BaseScan. (2025). *Base Network Daily Transactions Chart.* Retrieved from https://basescan.org/chart/tx
- Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. *Scalable zero knowledge with no trusted setup.* CRYPTO 2019.
- BC-IFSA Journal. (2024). *Kinexys Digital Assets: Tokenization at Scale.* Retrieved from https://bc-ifsa-journal.com/p_bc_17.html
- Bitansky N., Chiesa A., Ishai Y., Ostrovsky R., Paneth O. *Succinct non-interactive arguments via linear interactive proofs.* TCC 2013.
- Bois A., Cascudo I., Fiore D., Kim D. *Flexible and efficient verifiable computation on encrypted data.* PKC 2021.
- Boneh D., Sahai A., Waters B. *Functional encryption: Definitions and challenges.* TCC 2011.
- Brakerski Z., Gentry C., Vaikuntanathan V. *(Leveled) fully homomorphic encryption without bootstrapping.* ACM Trans. Comp. Theory, 2014.
- Buterin V. (2024). *The Three Transitions.* Ethereum Foundation Blog. Retrieved from https://vitalik.eth.limo/general/2024/10/23/futures4.html
- Central Banking. (2024). *CBDC Transactions Hit Seven Trillion Yuan, PBoC Official Says.* Retrieved from https://www.centralbanking.com/central-banks/currency/7962276/cbdc-transactions-hit-seven-trillion-yuan-pboc-official-says
- Chillotti I., Joye M., Paillier P. *Programmable bootstrapping enables efficient homomorphic inference of deep neural networks.* CSCML 2021.
- CoinDesk. (2023). *JPMorgan Handles $1 Billion Transactions Daily in Digital Token JPM Coin.* Retrieved from https://www.coindesk.com/business/2023/10/26/jpmorgan-handles-1b-transactions-daily-in-digital-token-jpm-coin-bloomberg
- Damgaard I., Pastro V., Smart N. P., Zakarias S. *Multiparty computation from somewhat homomorphic encryption.* CRYPTO 2012.
- Etherscan. (2025). *Ethereum Daily Transactions Chart.* Retrieved from https://etherscan.io/chart/tx

- Fiore D., Gennaro R., Pastro V. *Efficiently verifiable computation on encrypted data.* ACM CCS 2014.
- Fiore D., Nitulescu A., Pointcheval D. *Boosting verifiable computation on encrypted data.* PKC 2020.
- Gabizon A., Williamson Z. J., Ciobotaru O. *PLONK: permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge.* IACR Cryptol. ePrint Arch., 2019.
- Gailly N., Melissaris K., Romailler Y. *tlock: Practical timelock encryption from threshold BLS.* IACR Cryptol. ePrint Arch., 2023.
- Gentry C. *A fully homomorphic encryption scheme.* PhD thesis, Stanford University, 2009.
- HydraDX. (2025). *Omnichain Fungible Token (OFT) Standard Documentation.* Retrieved from https://docs.hydradx.io
- Horizen Labs. (2025). *Horizen Tokenomics Whitepaper.*
- Knabenhans C., Viand A., Merino-Gallardo A., Hithnawi A. *VFHE: Verifiable fully homomorphic encryption.* WAHC 2024.
- LayerZero Labs. (2025). *Stargate V2 Overview.* Retrieved from https://docs.stargate.finance
- Pang Q., Zhu J., Möllering H., Zheng W., Schneider T. *BOLT: privacy-preserving, accurate and efficient inference for transformers.* IEEE SP 2024.
- Pass R., Shi E., Tramer F. *Formal abstractions for attested execution secure processors.* EUROCRYPT 2017.
- Polygon. 2022. *Plonky2*. Retrieved from https://github.com/mir-protocol/plonky2
- Sabt M., Achemlal M., Bouabdallah A. *Trusted execution environment: What it is, and what it is not.* IEEE TrustCom/BigDataSE/ISPA 2015.
- Secret Network. (2024). *SecretVM and Confidential Smart Contracts.* Retrieved from https://docs.scrt.network
- Tan S., Knott B., Tian Y., Wu D. J. *CryptGPU: Fast privacy-preserving machine learning on the GPU*. IEEE SP 2021.
- Tassa T. *Hierarchical threshold secret sharing.* TCC 2004.
- Thibault L. T., Walter M. *Towards verifiable FHE in practice: Proving correct execution of TFHE's bootstrapping using Plonky2.* IACR Cryptol. ePrint Arch., 2024.
- Thrive Protocol. (2025). *Thrive x Horizen: Funding the Future of Privacy-First Applications.* Retrieved from https://horizen.thrive.xyz