Overcast Protocol: Technical Architecture for Confidential Interchain Settlement

Feb 25, 2026

Contents

1 Abstract

This paper presents the technical architecture of the Overcast Protocol, a decentralized protocol designed to facilitate private, regulatory-compliant interchain settlement of commercial transactions and other types of transactions facilitated by stable coins. By integrating Galactica's Identity Virtual Machine (IVM) with the Aztec Network's Noir-based privacy execution environment, Overcast introduces a programmable compliance layer for digital assets. We detail the system's core components: a guardian-centric Zero-Knowledge (ZK) KYC framework, a (m, n) threshold disclosure mechanism utilizing Shamir's Secret Sharing (SSS), and an extension of Aztec's AIP-20 token standard to support Real-World Asset (RWA) compliance. Based on this private and compliant foundation, Overcast serves the protocol cross-chain using Native L1↔L2 messages, atomic swaps and x402 payment facilitators.

2 Introduction

Public blockchain protocols suffer from the "Transparency Tax"—a fundamental exposure of transaction metadata that renders them unsuitable for use-cases requiring private transaction settlement, such as many institutional transactions or commerce: for obvious reasons, visibility into payroll, supply chain pricing, or treasury movements constitutes a significant risk.

Overcast Protocol addresses this by providing a private settlement layer. Unlike traditional privacy protocols, Overcast embeds compliance directly into the cryptographic circuits, enabling Auditability-on-Demand and broader kinds of selective disclosures while shielding sensitive information from public view.

3 ZK Identity and Compliance Framework

The identity layer utilizes a modular ZK KYC system to bridge off-chain legal audits with on-chain anonymity.

3.1 Guardian-Led Registry

The system employs a trusted layer of **Guardians** responsible for traditional PII (Personally Identifiable Information) verification.

1. **Attestation:** Guardians commit hashed KYC records to a Merkle Tree on-chain.
2. **Proof of Existence:** Users generate ZK proofs demonstrating membership in the "Guardian Set" without revealing the specific leaf or underlying identity documents.
3. **Indexed Merkle Trees for Revocation:** The protocol utilizes Indexed Merkle Trees to manage revocation lists. This enables efficient non-membership proofs, allowing the system to verify that a user's identifier is not currently blacklisted or revoked without disclosing the identifier itself.

3.2 Tiered Compliance Guards

The Overcast token contract implements modular “Compliance Guards” that evaluate every transfer against a progressive four-tier hierarchy:

1. **Level 0 (Permissionless):** Standard ERC20-style transfer logic without additional compliance overhead.

2. **Level 1 (Existence Verification):** Requires a ZK proof demonstrating that the user possesses a valid record commitment within a Guardian’s registry. This confirms “KYC has been performed” without validating specific attributes.

3. **Level 2 (ZK Attribute Verification):** Involves zero-knowledge requirement checks against the underlying KYC data. Users generate ZK proofs to demonstrate compliance with specific criteria—such as **Age $\geq$ 18** or **Non-Sanctioned Status**—without disclosing raw data or PII.

4. **Level 3 (Active Monitoring & Disclosure):** Requires Level 1 and 2 verification and mandates the encryption of transfer metadata (amount, recipient, and specific identifiers) to the issuer’s public key. This supports regulatory requirements for high-stakes audits and fraud investigations.

4 Programmable Selective Disclosure Framework

Confidentiality in decentralized settlement is a fundamental requirement for the secure exchange of value and information. However, absolute anonymity is often incompatible with the auditability and compliance standards required for commercial, institutional, and legal processes—of which financial Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations are prominent examples. Overcast resolves this tension through **Selective Disclosures**, allowing for “Auditability-on-Demand” across a wide range of settlement use cases.

4.1 The Selective Disclosure Mechanism

Selective disclosure is the cryptographic process of revealing specific portions of private data to authorized parties during the execution of a private transaction. In the Overcast Protocol, this occurs atomically on the Aztec blockchain. When a user settles a payment or interacts with a compliant contract, the ZK proof verifies their identity while simultaneously disclosing the required metadata (e.g., name or unique identifier) to a designated recipient.

Key properties of these disclosures include:

1. **Programmable Configuration:** The disclosure logic is governed by an application specific disclosure smart contract. It defines exactly *what* is disclosed, *who* receives it, and under what *conditions*.

2. **Trustless Transparency:** Users can inspect the disclosure contract’s source code on-chain. Unlike legacy Web2 systems where data processing is opaque, Overcast users

know exactly how their PII is being handled before signing a transaction.

3. **Verification Rigor:** Every disclosure is verified for validity by Aztec's ZK-SNARK transaction verification. This ensures that the disclosed data is cryptographically tied to the user's original KYC certificate and that the recipient is the one authorized by the contract.

4.2 Modular Disclosure Architectures

The protocol utilizes a modular DisclosureInterface, allowing the CertificateRegistry to call external contracts for varied compliance needs. Overcast provides three standardized implementations:

1. **No Disclosure:** For non-regulated use cases requiring maximum privacy.
2. **Basic Direct Disclosure:** One-to-one data sharing.
3. **Threshold Disclosure (Shamir's Secret Sharing):** Multi-party data sharing for institutional-grade security.

4.3 Basic Direct Disclosure

The BasicDisclosure module represents the simplest form of on-chain auditability. Upon transaction execution, the contract emits a BasicDisclosureEvent containing specific fields—such as the unique_id of the certificate and the issuing Guardian.

These events are emitted as encrypted logs on the Aztec Network. Only the designated recipient, possessing the correct decryption key, can access the data via standard client-side libraries (Aztec.js). This identifier allows the recipient to correlate the transaction with a specific user and, if necessary, query the original Guardian for additional legal documentation.

4.4 Threshold Disclosure via Shamir's Secret Sharing

For high-value transactions or sensitive institutional use cases, Overcast implements a (t, n) threshold disclosure scheme based on Shamir's Secret Sharing (SSS). This prevents any single entity from unilaterally deanonymizing a user, providing a "multi-signature" approach to data privacy.

4.4.1 Mathematical Implementation

The system constructs a polynomial $p(x)$ of degree $m - 1$, where the constant term $p(0)$ is the secret (e.g., the user's legal surname or tax ID). To ensure cryptographic robustness within Noir:

1. **Deterministic Coefficients:** Higher-degree coefficients are derived using a Poseidon2 hash of a coefficient_seed, which combines the transaction context and the certificate unique_id. This ensures that even for the same user, different transactions generate unique, unlinkable shards.

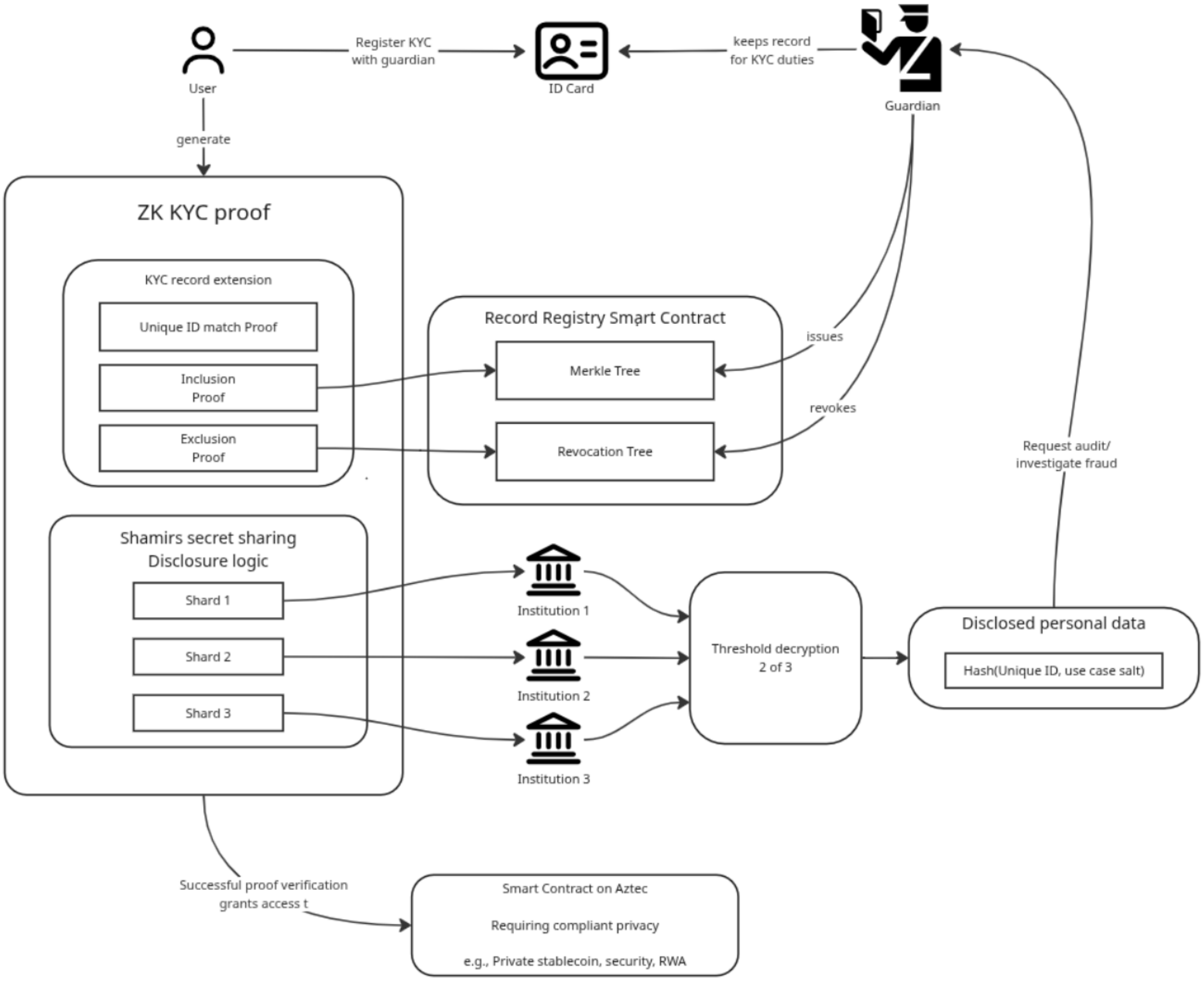
User
Register KYC with guardian
ID Card
keeps record for KYC duties
Guardian
generate
ZK KYC proof
KYC record extension
Unique ID match Proof
Inclusion Proof
Exclusion Proof
Record Registry Smart Contract
Merkle Tree
Revocation Tree
issues
revokes
Request audit/ investigate fraud
Shamirs secret sharing Disclosure logic
Shard 1
Shard 2
Shard 3
Institution 1
Institution 2
Institution 3
Threshold decryption 2 of 3
Disclosed personal data
Hash(Unique ID, use case salt)
Successful proof verification grants access t
Smart Contract on Aztec
Requiring compliant privacy
e.g., Private stablecoin, security, RWA

Figure 1: Overview

2. **Shard Distribution:** The secret is split into n shards. Each recipient i receives a point $(x_i, p(x_i))$ delivered via an on-chain constrained message.
3. **Quorum Reconstruction:** A quorum of at least m institutions must collaborate to reconstruct the polynomial and reveal $p(0)$. This provides redundancy against lost keys and collective defense against unauthorized surveillance.

4.5 Available Data and Context

Disclosure implementations have access to both the static ZK Certificate data (Name, DOB, Residency) and dynamic **Context Data**. The context is passed by the calling application and can include transaction-specific metadata such as the stablecoin amount, the destination address, or an invoice reference. This allows regulators or auditors to link a physical identity to a specific economic activity within the private execution environment.

4.6 On-Chain vs. Off-Chain Disclosure Strategies

While Overcast focuses on on-chain disclosures for atomic verification, the architecture supports off-chain alternatives.

1. **On-Chain Disclosure:** Ideal for real-time compliance checks and automated settlement triggers. It leverages the blockchain for data availability and delivery.
2. **Off-Chain Disclosure:** Can be implemented at the application front-end to mitigate "store now, decrypt later" risks associated with long-term on-chain storage of encrypted PII. In this model, the user discloses a one-time nonce on-chain that authorizes the recipient to request data from the Guardian through a secure, off-chain communication channel.

5 Settlement Layer: The Private Stablecoin Wrapper

The Overcast settlement layer extends the **Aztec AIP-20** token standard with features derived from the **CMTA (Capital Markets Technology Association)** standard to support institutional security requirements.

5.1 The Portal Pattern and Yield Routing

The protocol employs a **Portal Pattern** for bridging public L1 assets (e.g., USDC, USDT) into the private L2:

1. **L1 Escrow:** Public assets are locked in an Ethereum portal contract.
2. **L2 Minting:** The corresponding amount is minted as a private synthetic note on Aztec.
3. **Capital Efficiency:** Underlying L1 funds are routed into yield-bearing protocols (e.g., **Ethena**). This ensures that the private synthetic remains pegged to its public counterpart while generating staking returns for the holder or protocol.

6 Cross-Chain Bridging and Settlement Architecture

The Overcast Protocol is designed to bridge the gap between public liquidity on various L1/L2 chains and a private, compliant settlement layer on Aztec. To achieve this, the protocol employs a modular bridging and settlement architecture that prioritizes privacy, capital efficiency, and user experience.

Note: The cross-chain settlement design is currently in an early development phase. The concepts described below are subject to refinement as the protocol proceeds from design to functional prototype and subsequent iterations.

6.1 1. Asynchronous Asset Interoperability (The Portal Pattern)

Overcast utilizes the **Portal Pattern** to facilitate asset movements between the public L1/L2 ecosystem and the private Aztec environment. This architecture treats the bridge not just as a one-way entry point, but as an asynchronous messaging system capable of multi-hop logic.

6.1.1 The (L2 →) L1 → L2 Recursive Settlement Flow

While standard entry relies on L1 escrow, Overcast focuses on an interaction model where actions on Aztec trigger L1 state changes that then report back to L2. Crucially, because the settlement hub is Ethereum (L1), messages can be chained from other popular networks (such as Arbitrum, Optimism, or Galactica) through Ethereum's native messaging or third-party protocols like Hyperlane before being "pulled" into Aztec.

1. **L2 Emission (Outbox):** An L2 contract emits a L2ToL1Msg (e.g., a withdrawal request or a yield-rebalancing instruction). This message is scoped to the specific L2 contract and is added to the L2 outbox upon rollup finality.
2. **L1 Execution & Chaining (Portal):** The L1 Portal contract "pulls" the message from the L1 outbox. This triggers an L1 action, such as releasing ERC20 tokens or interacting with a yield protocol. In multi-chain scenarios, this step can involve receiving a message from an external L2 (e.g., via Arbitrum Orbit or Hyperlane) that is then processed by the portal on Ethereum.
3. **L1 Feedback Loop (Inbox):** If the action requires a state update on L2 (e.g., confirming a successful swap or re-wrapping updated yield amounts), the Portal contract emits an L1ToL2Msg. This effectively acts as the final hop for any message originating from either Ethereum or a chained external L2.
4. **L2 Consumption (Private):** The recipient on Aztec generates a ZK proof to consume this message from the L2 inbox. By "pulling" rather than "pushing" the message, the protocol hides the link between the L1 transaction and the specific L2 address, maintaining the privacy of the synthetic note holder.

6.1.2 Privacy Precaution: Decoupling Payment and Delivery

When executing on-chain or DeFi commerce using private stablecoins, a critical privacy risk arises if the delivery of the purchased asset or service is directly and immediately triggered by the payment. Since asset delivery on a public blockchain is observable, an immediate correlation between a private payment and a public delivery could allow observers to de-anonymize the transaction details.

To mitigate this, the protocol necessitates a logical **decoupling and temporal delay** between the settlement of funds and the fulfillment of the service. By introducing non-deterministic delays or fulfilling delivery through asynchronous off-chain processes, the protocol ensures that the public metadata of the delivery cannot be trivially linked back to the private financial transaction on Aztec.

6.2 2. Interchain Settlement via Atomic Swaps (TRAIN Protocol)

For transactions originating from chains outside of the Ethereum ecosystem (e.g., Solana, Base, or Galactica), Overcast integrates the **TRAIN PreHTLC (Pre-Hashed Timelock Contract)** flow.

6.2.1 Fast, Secure Interchain Swaps

Unlike traditional bridges that require long waiting periods for finality, the TRAIN PreHTLC mechanism enables rapid atomic swaps:

1. **Mechanism:** A user locks funds on a source chain to trigger a corresponding private transfer on Aztec.
2. **Solvers:** Automated backends (solvers) facilitate the swap, providing the liquidity on the destination chain.
3. **Trustlessness:** The transaction is atomic; if the swap is not fulfilled, the user's funds are recovered via the timelock mechanism.

This allows a user on Solana to settle a payment with an Overcast merchant on Aztec in a seemingly unified flow, significantly reducing the friction of onboarding to the private environment.

6.3 3. High-Throughput Settlement: x402 & State Channels

To support commercial-scale transaction volumes and micro-payments (e.g., for AI compute or API access), Overcast leverages **x402 Facilitators**.

6.3.1 Facilitated Batching

Facilitators act as specialized nodes that streamline the settlement process:

1. **Off-Chain Invoicing:** Communication between buyer and seller occurs off-chain via the x402 standard (HTTP 402 Payment Required).
2. **State Channels:** Facilitators can operate state channels by escrowing user funds in private smart contracts. This allows for nearly instant, zero-cost micro-transactions.
3. **Signature Batching:** Multiple transaction signatures are collected by the facilitator and batched into a single on-chain settlement. This satisfies the token contract's compliance hooks while drastically reducing gas costs per transaction.

6.4 4. Unified Interchain User Experience

Overcast aims to abstract the complexities of Aztec's account management for users coming from other chains.

6.4.1 Account Abstraction & Onboarding

Leveraging Aztec's native account abstraction, the protocol supports authentication from existing sources:

1. **EVM/Solana Compatibility:** Users can authorize Aztec transactions using their existing wallets or passkeys.
2. **Single-Transaction Onboarding:** The protocol is designing flows where "depositing from L1" and "private transfer to merchant" are composed into a single user-experience action.
3. **Note Discovery:** To maintain privacy while ensuring users can find their funds, Overcast implements custom note discovery mechanisms that allow recipients to identify their private notes without leaking metadata to the sequencer.

7 Agentic Commerce: x402 and AP2

Overcast is designed for autonomous AI agents acting as economic actors through the **x402 (HTTP 402 Payment Required)** and **AP2 (Agent Payments Protocol)** standards.

7.1 x402 Payment Workflow

The x402 module handles the logic for private invoicing and settlement:

1. **Request:** Agent requests a resource and receives a 402 header.
2. **Proof Generation:** The agent generates a standard ownership proof, a ZK KYC compliance proof, and a non-membership (non-frozen) proof.
3. **Execution:** The payment is submitted as a signed payload via **Authorization Witnesses (AuthWit)**, satisfying the token contract's compliance hooks while maintaining the parent entity's privacy.

7.2 Delegated KYC (Know Your Agent)

Agents inherit compliance through their "Parent" identity. The parent issues an AuthWit that cryptographically restricts the agent's spending limits, duration, and counterparties, allowing agents to operate autonomously without requiring an independent KYC process.

The AuthWit technically allows a smart contract to execute a private transaction for someone else. The user can prepare the AuthWit proving compliance and spending and hand it over to the agent to use it when transacting on-chain.

8 Conclusion

The Overcast Protocol provides a robust technical solution to the "Transparency Tax" by merging ZK-based identity with confidential settlement. Through the use of Noir smart contracts, SSS-based threshold disclosure, and interchain state replication, Overcast enables a new class of compliant, private stablecoins. This architecture serves as the foundational layer for both human and agentic commerce in an increasingly multi-chain financial ecosystem.