OVERLAYER

A Non-Custodial Infrastructure Protocol for Stablecoins

Non-rebasing stablecoin overlays with separate, opt-in on-chain yield participation.

Version 1.0

April 30, 2026

contact@overlayer.fi

This document is informational and technical. It is not legal, tax, financial, investment, regulatory, or compliance advice.

Legal and Risk Notice

This document (the "Whitepaper") is provided for informational and technical purposes only. It describes a proposed smart-contract protocol architecture, the intended Version 1.0 deployment scope, and relevant assumptions, limitations, and risks. It does not constitute and shall not be interpreted as an offer, solicitation, recommendation, invitation, or inducement to acquire, purchase, sell, subscribe for, or otherwise transact in any token, digital asset, security, financial instrument, deposit, payment instrument, or regulated product. It is not legal, tax, accounting, financial, investment, regulatory, or compliance advice.

No representation, warranty, undertaking, or assurance is made regarding the accuracy, completeness, regulatory treatment, future performance, availability, security, liquidity, market price, adoption, or economic outcome of the protocol or any related asset. Any forward-looking statements, roadmap items, deployment plans, governance transitions, future modules, or ecosystem programs are inherently uncertain and subject to change.

The protocol does not guarantee returns, yields, price stability, market liquidity, regulatory classification, availability of any interface, or successful redemption in all conditions. Any yield-related effects described in this Whitepaper are variable, may be zero, may be interrupted, and depend on external venue conditions, protocol parameters, and other risks. Users interact with the protocol at their own risk.

Overlayer is designed so that users interact with smart contracts rather than depositing assets with a traditional custodian. However, Version 1.0 includes disclosed launch-stage administrative controls, upgrade mechanisms, emergency controls, per-block limits, external venue dependencies, cross-chain messaging dependencies, and hosted-interface constraints. Accordingly, references to non-custodial or rules-based operation should be read in that technical and limited sense, not as a statement that no person, entity, administrator, governance process, interface operator, external venue, issuer, or infrastructure provider can affect user experience or outcomes.

The core smart contracts may be accessible without account registration. Hosted interfaces, access providers, integrators, wallets, exchanges, front-end operators, or jurisdiction-specific deployments may apply additional terms, disclosures, eligibility checks, sanctions controls, geographic restrictions, wallet screening, access limitations, or operational controls. The availability of a smart contract on a public blockchain does not mean that any person is legally permitted to interact with it in every jurisdiction or circumstance.

Regulatory treatment of crypto-assets, smart-contract protocols, stablecoin-related products, governance tokens, staking mechanisms, token sales, airdrops, cross-chain transfers, and DeFi interfaces varies by jurisdiction and may evolve over time. Nothing in this Whitepaper should be read as a legal conclusion regarding the classification, permissibility, registration status, licensing status, tax treatment, or compliance status of the protocol, any token, any interface, any participant, or any activity.

Where this document is used in connection with an offer to the public, admission to trading, token distribution, interface launch, or jurisdiction-specific communication, additional legal

review, formatting, disclosures, notifications, approvals, filings, restrictions, or amendments may be required. Local counsel should review the final version before publication or use in any regulated context.

This Whitepaper is non-normative except where expressly stated. In the event of any inconsistency between this Whitepaper and deployed smart contracts, the deployed smart contracts and their publicly verifiable behavior shall prevail. In the event of any inconsistency between this Whitepaper and applicable law, applicable law shall prevail.

Regulatory Review Notice

This Whitepaper has not been approved by any competent authority in any Member State of the European Union, the United States, the United Kingdom, the Cayman Islands, the British Virgin Islands, or any other jurisdiction. The person or entity responsible for any offer, admission to trading, interface, token distribution, or user-facing communication is responsible for ensuring that such activity and communication comply with applicable law.

A crypto-asset, governance token, staking representation, or related digital asset may lose its value in part or in full, may not always be transferable, may not be liquid, and may not be covered by investor compensation schemes, deposit guarantee schemes, or similar protections. This Whitepaper does not constitute a prospectus, offering memorandum, regulated white paper, listing document, or other offer document under any specific legal framework unless expressly adopted and reviewed for that purpose.

Contents

Legal and Risk Notice **1**

Regulatory Review Notice . . . 2

Executive Summary **7**

Abstract **8**

1 Introduction **9**

1.1 Stablecoins as Settlement Infrastructure . . . 9

1.2 Design Constraints . . . 9

1.3 Overlayer's Design Response . . . 10

1.4 Regulatory-Aware Design Objectives . . . 10

2 Version 1.0 Deployment Scope **10**

2.1 Core Deployment . . . 10

2.2 Supported Assets . . . 11

2.3 External Yield Venue . . . 11

2.4 Receipt-Token Minting and Redemption . . . 11

2.5 Cross-Chain Transfer . . . 11

2.6 Governance and Launch Administration . . . 12

2.7 Upgradeability and Delay . . . 12

2.8 Blacklist Functionality . . . 12

2.9 Emergency Withdrawal . . . 12

2.10 Reserve Index Status . . . 13

3 System Model and Definitions **13**

3.1 Actors . . . 13

3.2 Assets . . . 14

3.3 State Variables . . . 14

3.4 Notation . . . 15

3.5 Core Accounting Principles . . . 15

3.6 Assumptions and Limitations . . . 15

4 Asset Model: Overlaid Assets **16**

4.1 Definition . . . 16

4.2 Non-Rebasing Settlement Design . . . 16
4.3 Not a Yield-Bearing Payment Balance . . . 16
4.4 Backing and Redeemability . . . 17
4.5 Scope and Non-Goals . . . 17

5 Protocol Architecture and Control Surface 17
5.1 Core Contracts . . . 17
5.2 Upgradeability . . . 18
5.3 Control Surface Matrix . . . 18
5.4 Emergency Venue Withdrawal . . . 19
5.5 Blacklist Functionality . . . 19
5.6 Governance Transition . . . 20

6 Core Protocol Operations 20
6.1 Minting with Underlying Stablecoins . . . 20
6.2 Minting with Receipt Tokens . . . 20
6.3 Redemption into Underlying Stablecoins . . . 21
6.4 Redemption into Receipt Tokens . . . 21
6.5 Redemption Under Liquidity Stress . . . 21
6.6 Staking . . . 22
6.7 Unstaking . . . 22

7 Staking and Yield Allocation 22
7.1 Source of Yield . . . 22
7.2 Realization and Allocation . . . 23
7.3 Share-Based Accounting . . . 23
7.4 Overyield Dynamics . . . 23
7.5 Exchange Rate Limitations . . . 23
7.6 Emergency Withdrawal and Yield Interruption . . . 24
7.7 No Automatic Holder Yield . . . 24

8 Cross-Chain Transfer Model 24
8.1 Ethereum as Core Backing Environment . . . 24
8.2 Omnichain Transfer Mechanics . . . 24
8.3 Messaging-Layer Risk . . . 24
8.4 No Independent Destination-Chain Backing . . . 25

9 Planned Auxiliary Module: Reserve Index **25**
9.1 Planned Purpose . . . 25
9.2 Planned Composition . . . 25
9.3 Risk Isolation . . . 26
9.4 Separate Disclosure Required . . . 26

10 Security and Risk Considerations **26**
10.1 Smart Contract Risk . . . 26
10.2 Upgrade and Administrative Risk . . . 26
10.3 Aave Risk . . . 26
10.4 Underlying Stablecoin Risk . . . 27
10.5 Receipt-Token Risk . . . 27
10.6 Liquidity and Redemption Risk . . . 27
10.7 Cross-Chain Risk . . . 27
10.8 Blacklist and Access Risk . . . 27
10.9 Regulatory Risk . . . 28
10.10Market and Integration Risk . . . 28

11 Governance and the OVER Token **28**
11.1 Launch Phase . . . 28
11.2 Future Governance . . . 28
11.3 OVER Token Role . . . 28

12 Conclusion **29**

Glossary **30**

A Mathematical Appendix: Share Accounting **31**
A.1 Definitions . . . 31
A.2 Exchange Rate . . . 31
A.3 Staking . . . 31
A.4 Unstaking . . . 31
A.5 Yield Allocation . . . 32
A.6 Normal-State Accounting Properties . . . 32

B Parameter Summary **33**
B.1 Core Parameters . . . 33

B.2 Minting and Redemption Parameters 33
B.3 Yield and Allocation Parameters 33
B.4 Governance Parameters 33
B.5 Interoperability Parameters 34
B.6 Parameter Mutability 34

References **35**

Executive Summary

Overlayer is a smart-contract protocol for wrapping supported stable-valued assets into non-rebasing overlaid assets. In Version 1.0, the protocol is intended to support USDC and USDT on Ethereum as the primary minting, redemption, and backing environment. The protocol may also enable transfer of supported tokens across additional chains through LayerZero-based omnichain functionality.

The protocol separates two functions that are often combined in DeFi products: settlement and yield participation. The base overlaid asset is designed as a transferable, non-rebasing ERC-20-compatible settlement representation. It does not automatically accrue yield merely by being held. Yield participation is separate, optional, and implemented through a share-based staking representation. This separation is a core design choice intended to preserve composability, reduce hidden accounting complexity, and avoid describing the base overlaid asset as an automatic yield-bearing payment instrument.

At launch, underlying assets are expected to be deployed into Aave as the sole external yield venue. Users may mint or redeem through supported underlying stablecoins or through supported Aave receipt-token representations. When redemption is settled in receipt-token form, users receive the relevant receipt-token representation rather than immediate raw underlying stablecoins. Ultimate conversion of such receipt tokens into the underlying stablecoin depends on Aave liquidity and other Aave-specific conditions.

Version 1.0 is not fully immutable or fully decentralized at launch. The contracts are expected to be upgradeable subject to specified constraints. Certain high-impact upgrades require a mandatory 14-day delay, which is intended to provide users with advance notice and an opportunity to exit before the relevant change becomes effective. Launch-stage administrative functions are expected to be controlled by a Foundation multisignature wallet. These controls include parameter changes, emergency withdrawal from Aave, and a disabled blacklist module that could only be activated after a 14-day upgrade delay. If activated, blacklist functionality could block affected wallets from interacting with Overlaid Assets.

The protocol is designed to avoid protocol-level borrowing, recursive leverage, off-chain hedging, discretionary minting, and direct issuer-paid yield on the base overlaid asset. It nevertheless depends on external systems and facts, including the solvency and operation of USDC and USDT issuers, Aave, Ethereum, LayerZero, administrative controls, and any hosted interfaces. The protocol does not eliminate stablecoin issuer risk, Aave risk, cross-chain risk, smart-contract risk, regulatory risk, governance risk, liquidity risk, or market risk.

This Whitepaper describes a technical architecture and a design posture. It does not assert that any asset, module, token, or activity is outside any legal or regulatory framework. The protocol has been designed with regulatory considerations in mind, including separation between settlement and opt-in yield participation, avoidance of automatic yield on base settlement balances, and avoidance of claims against a legal entity for fiat redemption. These design choices do not replace formal legal analysis.

Abstract

Overlayer is a non-custodial smart-contract protocol that wraps supported stable-valued assets into non-rebasing overlaid assets backed by protocol-controlled on-chain positions. The protocol is designed to preserve the underlying unit of account while moving accounting, minting, redemption, and optional yield participation into auditable smart-contract flows.

The base overlaid asset, denoted S^+, is a non-rebasing transferable token. It is not designed to pay yield solely by virtue of being held. Yield participation is separate and opt-in through a share-based staking representation, denoted sS^+, whose exchange rate relative to S^+ may increase when realized yield is allocated to the staking module. The protocol does not borrow, does not create recursive leverage, and does not rely on token emissions to fund protocol staking yield.

Version 1.0 is expected to support USDC and USDT on Ethereum, with Aave as the sole external yield venue at launch. Minting and redemption may be performed using supported underlying stablecoins or supported Aave receipt-token representations. Cross-chain transfer functionality is expected to be available at launch through LayerZero-based omnichain token mechanics, subject to separate messaging-layer risk.

The protocol includes disclosed launch-stage controls. Contracts are upgradeable within defined limits; certain high-impact changes require a 14-day delay. A Foundation multisignature wallet is expected to control administrative functions at launch. Blacklist functionality exists in the codebase but is disabled at launch and cannot be activated without the applicable delay. Emergency withdrawal from Aave may be used to reduce venue exposure but may interrupt or reduce yield.

This Whitepaper does not provide legal conclusions. It describes a protocol architecture designed around transparent accounting, unit-based backing, optional yield participation, and explicit risk disclosure. Specialist counsel should review the final publication, interfaces, token distributions, and user-facing communications before launch.

1. Introduction

Stablecoins are widely used as settlement assets in on-chain markets because they combine a familiar unit of account, broad liquidity, and operational simplicity. They are used in exchanges, money markets, liquidity pools, payments infrastructure, treasury management, and protocol-level accounting.

The design choices embedded in stablecoins therefore affect more than individual holders. They affect composability, liquidity routing, collateral design, and the reliability of higher-layer protocols that depend on stable settlement primitives.

1.1 Stablecoins as Settlement Infrastructure

The dominant stablecoin model relies on off-chain reserve management and issuer-administered contracts. This structure has proven useful for liquidity and market adoption, but it also embeds issuer-level controls, policy risk, freeze risk, and off-chain redemption dependencies into the settlement layer. Transfer restrictions and administrative interventions are not accidental edge cases; they are part of the design space for many fiat-backed stablecoins.

At the same time, stablecoins that are optimized for transferability do not automatically make on-chain capital productive for holders. Yield generated from off-chain reserves generally accrues outside the user's on-chain balance. Users who want on-chain yield often need to move stablecoins into separate venues, vaults, or applications, each with its own accounting and risk assumptions.

1.2 Design Constraints

A protocol that builds on existing stablecoins while attempting to improve on-chain utility must operate within several constraints:

1. It should preserve the unit exposure and broad usability of supported stablecoins rather than requiring users to adopt a new monetary unit.
2. It should keep base settlement balances simple, non-rebasing, and compatible with standard on-chain applications.
3. It should avoid protocol-level borrowing, recursive leverage, opaque off-chain hedging, and discretionary minting.
4. It should make yield participation explicit and optional rather than embedding yield into every transferable unit.
5. It should disclose administrative controls, external dependencies, and legal limitations rather than relying on absolute decentralization claims.

1.3 Overlayer's Design Response

Overlayer responds to these constraints through an overlaid asset model. Users may supply a supported stablecoin or a supported receipt-token representation and receive a non-rebasing overlaid asset. The overlaid asset is designed for transfer, settlement, and composability. Yield participation is separated into a distinct staking representation.

This architecture does not eliminate stablecoin issuer risk or external venue risk. Instead, it makes those dependencies explicit and seeks to constrain the protocol's own risk contribution. The protocol does not attempt to create a new synthetic dollar, does not guarantee fiat value, and does not promise yield. It defines a rules-based wrapping and optional staking architecture around supported stable-valued assets.

1.4 Regulatory-Aware Design Objectives

The protocol has been designed with several regulatory considerations in mind:

- The base overlaid asset is not designed to pay yield solely by being held.
- Yield participation requires an affirmative, opt-in staking action and produces a distinct staking representation.
- The protocol does not describe overlaid assets as fiat claims against the Foundation, developers, interface operator, or any legal entity.
- The protocol does not describe staking shares as deposits, debt instruments, profit-sharing interests, or guaranteed-return products.
- The Whitepaper avoids assertions about future value, token price, launch valuation, buybacks, or guaranteed economic outcomes.

These are design objectives, not legal conclusions. Whether any particular asset, token, interface, sale, airdrop, staking mechanism, or module is regulated depends on applicable law, jurisdiction, facts, distribution methods, user-facing communications, and implementation details.

2. Version 1.0 Deployment Scope

This section defines the intended Version 1.0 scope. Statements about later modules, future governance, or future chains should not be read as describing live protocol functionality unless expressly stated.

2.1 Core Deployment

Version 1.0 is intended to use Ethereum as the primary chain for minting, redemption, backing, and Aave integration. The supported underlying assets at launch are expected to be USDC and USDT only.

The protocol may allow token transfer across additional supported chains through LayerZero-based omnichain mechanics. Such transfers extend the portability of the relevant token representation but do not create independent backing reserves on destination chains unless a deployment expressly discloses otherwise.

2.2 Supported Assets

Each overlaid asset deployment is associated with a specific supported underlying asset. For Version 1.0:

Underlying Asset	Overlaid Asset	Launch Status
USDC	C+ or equivalent deployment ticker	Intended for Version 1.0
USDT	T+ or equivalent deployment ticker	Intended for Version 1.0

Final token symbols, contract addresses, supported chains, and integration parameters should be verified against the deployed contracts and official deployment notices.

2.3 External Yield Venue

Aave is intended to be the sole external yield venue at launch. Overlayer therefore inherits Aave-specific risks, including smart-contract risk, governance risk, liquidity risk, reserve risk, utilization risk, market risk, and the risk that Aave receipt tokens become impaired, illiquid, paused, or otherwise affected by Aave-specific conditions.

Future deployments may add or replace external venues only if disclosed through the relevant governance, upgrade, or parameter-change process. Such additions or replacements may materially alter the protocol's risk profile.

2.4 Receipt-Token Minting and Redemption

Version 1.0 is intended to support minting and redemption using supported Aave receipt-token representations from launch. A user may therefore interact with the protocol using either the supported underlying stablecoin or, where enabled, its supported Aave receipt-token representation.

Receipt-token settlement is not equivalent to guaranteed immediate delivery of raw underlying stablecoins. If a user receives a receipt-token representation, that user remains exposed to the external venue's rules and liquidity conditions when attempting to convert the receipt token into the underlying stablecoin.

2.5 Cross-Chain Transfer

Cross-chain transfer functionality is intended to be active at launch for supported tokens and supported chains. The protocol is expected to use LayerZero or another disclosed

omnichain messaging framework. Cross-chain transfer functionality introduces separate message-validation, endpoint, relayer, configuration, destination-chain, and operational risks.

2.6 Governance and Launch Administration

Governance through the OVER token is not expected to be live at initial protocol launch. Version 1.0 is expected to begin with a Foundation-controlled phase. Administrative functions are expected to be controlled by a Foundation multisignature wallet.

The eventual introduction of OVER or decentralized governance should not be read as guaranteed. Any future governance token, sale, airdrop, distribution, or governance process will require separate disclosures and legal review.

2.7 Upgradeability and Delay

The Version 1.0 contracts are expected to be upgradeable within defined limits. Certain high-impact or potentially dangerous changes require a mandatory 14-day delay before taking effect. This delay is intended to provide users with advance notice and an opportunity to exit if they disagree with the proposed change.

A delay mechanism reduces but does not eliminate upgrade risk. Users and integrators should monitor upgrade notices, governance announcements, contract events, and official disclosures.

2.8 Blacklist Functionality

Blacklist functionality exists in the codebase but is disabled at launch. Activation requires the applicable upgrade process and a 14-day delay. If activated, authorized roles may be able to blacklist or unblacklist wallets, and a blacklisted wallet may be blocked from performing actions involving Overlaid Assets, including transfer, minting, redemption, staking, unstaking, or cross-chain movement, depending on implementation details.

The existence of this module means that the protocol should not be described as providing unconditional access or absolute censorship resistance. The launch configuration and activation delay should be evaluated as part of the protocol's disclosed control surface.

2.9 Emergency Withdrawal

The protocol includes an emergency function that may withdraw funds from Aave if the Foundation multisignature wallet determines that venue exposure should be reduced. This function is intended to protect availability of principal within the protocol's own contracts during external venue stress. It may reduce or halt ongoing yield until assets are redeployed.

Emergency withdrawal is a risk-management tool, not a guarantee of loss prevention, continuous redemption, or uninterrupted yield.

2.10 Reserve Index Status

The Reserve Index is a planned auxiliary module and is not part of Version 1.0 core minting, redemption, backing, or staking accounting. It is expected to be integrated later and will require separate disclosure. Planned index composition and dependencies are summarized in Section 9 but should not be read as live Version 1.0 functionality.

3. System Model and Definitions

The following definitions are used throughout this Whitepaper.

3.1 Actors

Users. Users are wallet holders or smart contracts that interact with Overlayer contracts, interfaces, or integrations. Users may mint, redeem, transfer, stake, unstake, or otherwise use supported assets according to the rules of the relevant deployment. User access may be affected by hosted-interface conditions, jurisdictional restrictions, sanctions controls, wallet screening, contract-level controls, or external venue conditions.

Protocol Contracts. Protocol contracts are smart contracts implementing minting, redemption, transfer, staking, accounting, external venue interactions, limits, and related functions. Version 1.0 contracts are expected to be upgradeable subject to disclosed constraints and delay mechanisms.

Foundation. The Foundation is the governance or administrative vehicle expected to control certain launch-stage administrative functions through a multisignature wallet. References to the Foundation do not imply that the Foundation guarantees redemption, yield, price stability, liquidity, or legal classification.

Foundation Multisignature Wallet. The Foundation multisignature wallet is the launch-stage administrative controller for specified functions. It may control parameters, emergency functions, upgrades, and other disclosed controls. The multisignature structure reduces single-key risk but does not eliminate administrative or governance risk.

Official Interface. The official interface is a hosted front-end or access layer that may be operated by a service provider engaged by the Foundation. The official interface may impose terms of use, disclosures, eligibility requirements, sanctions screening, geographic restrictions, wallet screening, or other controls that are separate from the smart contracts.

External Venue. An external venue is an on-chain protocol integrated by Overlayer for a specific function. In Version 1.0, Aave is expected to be the sole yield venue.

Messaging Layer. A messaging layer is external cross-chain infrastructure used to coordinate token transfers across supported chains. In Version 1.0, LayerZero or another disclosed framework may serve this role.

3.2 Assets

Underlying Stablecoin (S). A supported stable-valued token accepted by a deployment for minting an overlaid asset. Version 1.0 is expected to support USDC and USDT only. The protocol does not guarantee the market value, peg, issuer solvency, transferability, or regulatory status of any underlying stablecoin.

Receipt-Token Representation (aS). A supported receipt-token representation of an underlying stablecoin, such as an Aave aToken or another disclosed venue receipt token. A receipt token represents rights or accounting within an external venue and is subject to that venue's rules and risks.

Overlaid Asset (S^+). A non-rebasing ERC-20-compatible token minted by the protocol against a supported underlying stablecoin or supported receipt-token representation. Each unit of S^+ represents a protocol-defined redemption relationship against aggregate backing for the relevant deployment, subject to contract rules, limits, external venue conditions, administrative controls, and applicable law.

Staked Representation (sS^+). A share-based staking representation issued when a user opts into yield participation by staking S^+. The amount of S^+ redeemable for a given amount of sS^+ depends on the current exchange rate R. Staking shares are not deposits, debt instruments, or claims on any legal entity.

OVER Token. OVER is expected to be a future governance coordination token. It is not live at initial protocol launch, is not required for core minting or redemption, and does not represent equity, ownership, debt, revenue rights, reserve rights, or claims on protocol assets. Tokenomics, sale terms, airdrops, and distribution mechanics are outside the scope of this Whitepaper.

3.3 State Variables

Total Unit Backing (U). The total quantity of backing attributable to a deployment, measured in units of the supported underlying asset or its supported receipt-token representation, according to protocol accounting. U is not a guarantee of fiat value.

Total Overlaid Supply (T^+). The total outstanding supply of S^+ across the relevant deployment and supported chains, subject to the supply accounting of the applicable cross-chain token framework.

Total Staked Supply (T_s^+). The total outstanding supply of sS^+ shares.

Exchange Rate (R). The conversion rate between sS^+ shares and S^+, used for staking and unstaking calculations. Under normal accounting transitions, R changes only when realized yield is allocated to the staking module.

Realized Yield (Y). The portion of external venue returns realized by the protocol and made available for allocation according to disclosed parameters, net of applicable fees and subject to external venue conditions.

3.4 Notation

Symbol	Meaning
S	Supported underlying stablecoin
aS	Supported receipt-token representation of S
S^+	Non-rebasing overlaid asset
sS^+	Share-based staking representation
U	Total unit backing attributed to the deployment
T^+	Total overlaid asset supply
T_s^+	Total staking share supply
R	Exchange rate between sS^+ and S^+
Y	Realized yield allocated under protocol rules
t	Discrete accounting event index

3.5 Core Accounting Principles

The protocol is designed around the following accounting principles:

1. **Unit-Based Backing.** Backing is tracked in units of the supported underlying asset or supported receipt-token representation. This does not guarantee any fiat price, market price, or peg.
2. **Contract-Defined Redemption.** Redemption follows contract-defined rules and may settle in the supported underlying stablecoin or supported receipt-token representation, subject to limits, venue conditions, controls, and deployment configuration.
3. **No Protocol-Level Borrowing.** The protocol does not borrow assets or use recursive leverage to generate yield. External venues may involve lending-market risks, including borrower and utilization risk.
4. **Separate Yield Accounting.** Holding the base overlaid asset does not automatically generate yield. Yield participation requires a separate staking action and is reflected through share-based accounting.
5. **Explicit Controls.** Upgrade, emergency, limit, and blacklist-related controls are disclosed rather than treated as nonexistent.

3.6 Assumptions and Limitations

The protocol relies on assumptions that are outside its control, including:

- the continued operation and solvency of supported stablecoin issuers;
- the transferability and market acceptance of supported underlying assets;
- Aave smart-contract operation, liquidity, governance, and receipt-token behavior;
- Ethereum liveness, finality, and execution correctness;

- LayerZero or other messaging-layer security and configuration;
- responsible operation of launch-stage administrative controls;
- legal permissibility of user interactions in relevant jurisdictions.

Failure of an assumption may delay, impair, alter, or prevent specific operations and may cause economic loss. Internal accounting consistency does not guarantee external venue solvency, market price, or legal enforceability.

4. Asset Model: Overlaid Assets

Overlaid Assets are the primary base tokens issued by the protocol. They are designed to preserve the unit exposure of the supported underlying stablecoin while changing how custody, transfer, accounting, and optional yield participation are organized on-chain.

4.1 Definition

An Overlaid Asset (S^+) is a non-rebasing ERC-20-compatible token minted by Overlayer in exchange for a supported underlying stablecoin S or supported receipt-token representation aS. It represents a contract-defined redemption relationship against the aggregate backing of the relevant deployment.

S^+ is not a new fiat currency, is not legal tender, is not a bank deposit, is not an e-money account, and is not an unconditional claim against the Foundation, developers, front-end operator, stablecoin issuer, Aave, or any other legal entity. Its behavior is determined by the deployed contracts, external venue conditions, administrative controls, and applicable law.

4.2 Non-Rebasing Settlement Design

The base overlaid asset is non-rebasing. Its wallet balance does not increase merely because the protocol earns yield. This design is intended to preserve compatibility with wallets, automated market makers, lending markets, payment flows, accounting systems, and other applications that expect standard ERC-20 behavior.

Because S^+ does not automatically accrue yield, integrators do not need to track a changing exchange rate when integrating the base token. Yield participation is isolated in the staking representation described in Section 7.

4.3 Not a Yield-Bearing Payment Balance

Holding S^+ alone does not entitle the holder to receive protocol yield. A user who wants exposure to protocol-allocated yield must affirmatively stake S^+ into the staking module and receive sS^+ shares. This separation is central to the protocol design.

The protocol should not be marketed as providing passive stablecoin yield merely for holding a base settlement asset. Descriptions of yield should be limited to optional staking mechanics,

should state that yield is variable and may be zero, and should identify the relevant external venue and fee parameters.

4.4 Backing and Redeemability

Overlaid Assets are intended to be backed on an aggregate unit basis by protocol-controlled positions consisting of supported underlying assets and/or supported receipt-token representations. The protocol's backing relationship is not a fiat-value guarantee. If an underlying stablecoin depegs or loses market value, the corresponding overlaid asset remains exposed to that underlying asset's risk.

Redemption may settle in the underlying stablecoin or, where enabled, in the supported receipt-token representation. If redemption settles in receipt-token form, the user's ability to convert that receipt token into underlying stablecoins depends on the external venue and may be affected by liquidity, utilization, pauses, governance, or impairment.

4.5 Scope and Non-Goals

Overlaid Assets are not intended to:

- eliminate issuer-level risk of USDC, USDT, or any other supported stablecoin;
- guarantee fiat value, peg stability, market price, or liquidity;
- guarantee immediate redemption into raw underlying stablecoins in all conditions;
- eliminate Aave, Ethereum, LayerZero, governance, administrative, or smart-contract risk;
- provide unconditional access or absolute censorship resistance;
- create an issuer obligation to redeem for legal currency.

The intended role of S^+ is narrower: a non-rebasing, transferable, contract-defined representation of supported stablecoin exposure, with optional and separate yield participation.

5. Protocol Architecture and Control Surface

The protocol architecture consists of core contracts, external integrations, administrative controls, and optional modules. This section describes both the technical components and the control surfaces that may affect user outcomes.

5.1 Core Contracts

OverlayerWrap. `OverlayerWrap` is the issuance, redemption, and transfer module for a specific overlaid asset deployment. It mints S^+ when users supply supported assets and burns S^+ when users redeem. It may also implement LayerZero OFT or similar omnichain transfer functionality.

StakedOverlayerWrap. `StakedOverlayerWrap` implements the staking module. It is expected to follow ERC-4626-style share accounting, where users deposit S^+ and receive sS^+ shares. The staking module does not modify balances of unstaked S^+.

OverlayerBacking. `OverlayerBacking` manages backing positions and interactions with the external yield venue. In Version 1.0, it is expected to interact with Aave. It receives supported assets, supplies them to Aave where configured, holds or accounts for receipt-token positions, and makes realized yield available for allocation.

Rewards or Allocation Dispatcher. A dispatcher or allocation component may route realized yield according to protocol parameters, including allocations to staking and other disclosed destinations. Such routing is subject to parameter and governance risk.

5.2 Upgradeability

Version 1.0 contracts are expected to be upgradeable subject to defined limits. Upgradeability enables bug fixes, security responses, integration changes, and parameter updates. It also introduces risk because future code can change protocol behavior.

Certain high-impact or dangerous changes require a mandatory 14-day delay. The delay is intended to provide notice and an opportunity for users to exit before such changes become active. The delay does not guarantee that all users will see the notice, understand the change, be able to exit under market or venue conditions, or avoid all impact.

5.3 Control Surface Matrix

The following table summarizes the expected launch-stage control surface. Actual deployed contracts and official deployment notices should be treated as authoritative.

Control	Expected Controller at Launch	Delay	Purpose	User-Facing Risk
Contract upgrades	Foundation multisignature wallet	14 days for high-impact changes	Security maintenance, bug fixes, integration changes	Future code may change behavior; users must monitor notices
Per-block mint limits	Foundation multisignature wallet	Parameter-specific	Reduce short-term manipulation and flash-loan-driven issuance risk	Throughput may be limited during high demand
Per-block redemption limits	Foundation multisignature wallet	Parameter-specific	Reduce rapid liquidity drainage and manipulation risk	Large or urgent redemptions may be delayed

Control	Expected Controller at Launch	Delay	Purpose	User-Facing Risk
Emergency withdrawal from Aave	Foundation multisignature wallet	Expected to be callable when needed	Reduce exposure to external venue risk	Yield may stop or decrease; action depends on admin judgment
Yield allocation parameters	Foundation multisignature wallet or future governance	Parameter-specific	Set allocation of realized yield and protocol fees	Staker yield may change; fees may reduce allocation
Team, treasury, or recipient addresses	Foundation multisignature wallet or future governance	Parameter-specific	Operational routing and treasury management	Misconfiguration or governance capture risk
Blacklist module activation	Foundation multisignature wallet via upgrade process	14 days	Legal, sanctions, compliance, or emergency contingency	After activation, access may become restricted for affected wallets
Wallet blacklist or deblacklist after activation	Authorized role under activated module	Immediate once module is active	Enforce activated blacklist controls	Affected wallets may be blocked from all Overlaid Asset actions

5.4 Emergency Venue Withdrawal

The emergency withdrawal function is intended to withdraw funds from Aave when external venue conditions appear to present elevated risk. The function may move funds back into protocol-controlled contracts and reduce exposure to the external venue. It may also halt or reduce yield until assets are redeployed.

This mechanism should be understood as a risk-reduction control, not a guarantee. It relies on timely detection, administrator judgment, successful transaction execution, and the availability of assets for withdrawal from the external venue.

5.5 Blacklist Functionality

Blacklist functionality is disabled at launch. It cannot be activated without the applicable upgrade process and 14-day delay. If activated, it may allow authorized roles to block wallets from performing actions involving Overlaid Assets. The precise scope should be verified against deployed code.

This design reflects a trade-off between legal/compliance contingency planning and neutrality. The presence of a disabled but activatable blacklist module should be considered by users, integrators, and governance participants when assessing the protocol's control surface.

5.6 Governance Transition

Overlayer is expected to begin with a Foundation-controlled launch phase. Future governance may be introduced later through the OVER token or other mechanisms. Until such transition is deployed and effective, governance should not be described as decentralized or live.

Any transition to governance should include disclosures regarding voting power, quorum, timelocks, delegation, emergency authority, parameter scope, upgrade rights, conflicts of interest, and legal responsibilities.

6. Core Protocol Operations

This section describes minting, redemption, staking, and unstaking. Each operation is implemented through smart contracts but remains subject to disclosed limits, external venue conditions, administrative controls, and applicable law.

6.1 Minting with Underlying Stablecoins

A user may mint S^+ by supplying a supported underlying stablecoin S to the relevant `OverlayerWrap` deployment.

A typical minting flow is:

1. The user approves and supplies S to `OverlayerWrap`.
2. The protocol transfers or accounts for the supplied asset in the relevant backing structure.
3. The protocol may supply the asset to Aave, where configured.
4. The protocol mints the corresponding amount of S^+ to the user, subject to limits and checks.

Minting is intended to occur at a deterministic unit ratio, subject to fees if any are disclosed. It does not depend on a price oracle to determine the fiat value of S.

6.2 Minting with Receipt Tokens

Where enabled, a user may mint S^+ by supplying a supported receipt-token representation aS. The protocol accounts for the supplied receipt-token position according to deployment rules. This allows users who already hold supported Aave receipt tokens to enter the overlaid asset system without first withdrawing to the underlying stablecoin.

Receipt-token minting depends on correct accounting of the relevant receipt token, including decimals, exchange-rate assumptions, and external venue behavior. Users remain exposed to

the external venue risk embedded in the receipt token.

6.3 Redemption into Underlying Stablecoins

A user may redeem S^+ by burning it under the rules of the relevant deployment. Where sufficient underlying stablecoin liquidity is available, the protocol may settle redemption in the supported underlying stablecoin.

A typical underlying redemption flow is:

1. The user submits a redemption transaction and burns S^+.
2. The protocol computes the contract-defined redemption amount.
3. The backing contract uses available balances or withdraws from Aave if necessary and possible.
4. The user receives the supported underlying stablecoin, subject to limits, venue conditions, and controls.

Redemption into underlying stablecoins is not guaranteed to be continuously available in all conditions. Aave utilization, liquidity constraints, venue pauses, stablecoin issuer actions, per-block limits, emergency controls, or other events may delay, limit, or alter settlement.

6.4 Redemption into Receipt Tokens

Where enabled, redemption may settle in supported receipt-token form. In such cases, the user receives the relevant receipt token rather than raw underlying stablecoins. This settlement path may remain available even when immediate withdrawal of the underlying stablecoin from Aave is constrained, depending on protocol balances and implementation.

Users receiving receipt tokens assume receipt-token risk. The market price of a receipt token may differ from the value implied by venue accounting, and conversion into the underlying stablecoin ultimately depends on the external venue and available liquidity.

6.5 Redemption Under Liquidity Stress

If Aave liquidity is insufficient for immediate withdrawal of the underlying stablecoin, direct redemption into the underlying may be delayed, limited, or unavailable. Receipt-token settlement may provide an alternative settlement path, but it does not remove Aave risk. A user who receives receipt tokens may need to wait for Aave liquidity, sell the receipt tokens in a secondary market, or otherwise manage the position independently.

Per-block limits may also restrict the rate at which minting or redemption can occur. These limits are intended to reduce manipulation and rapid liquidity-drainage risk but may affect user execution during stress.

6.6 Staking

Staking is an optional action through which a user deposits S^+ into the staking module and receives sS^+ shares. Staking is the only protocol-defined mechanism through which users participate in realized yield allocation.

A typical staking flow is:

1. The user approves and deposits S^+ into `StakedOverlayerWrap`.
2. The staking contract mints sS^+ shares based on the current exchange rate R.
3. The user's exposure shifts from base S^+ to a staking share whose redeemable amount in S^+ depends on R.

Staking is not a deposit with a legal entity, not a savings account, not a debt claim, and not a guaranteed-yield arrangement.

6.7 Unstaking

A user may redeem sS^+ shares for S^+ according to the current exchange rate R, subject to contract rules and any applicable controls.

A typical unstaking flow is:

1. The user submits an unstaking transaction and burns or redeems sS^+ shares.
2. The staking contract computes the corresponding S^+ amount using R.
3. The user receives S^+.

Unstaking from sS^+ to S^+ does not itself require withdrawal from Aave. Redeeming the resulting S^+ into underlying stablecoins or receipt tokens is a separate operation subject to the redemption conditions described above.

7. Staking and Yield Allocation

Overlayer separates settlement from yield. The base overlaid asset is non-rebasing and does not automatically accrue yield. Yield participation is optional and implemented through a distinct staking representation.

7.1 Source of Yield

In Version 1.0, yield is expected to originate exclusively from supplying supported assets to Aave. Yield depends on Aave market conditions, including borrower demand, utilization, reserve parameters, incentives, and governance decisions. The protocol does not create yield internally and does not use OVER emissions to fund protocol staking yield.

Yield may be positive, zero, interrupted, reduced by fees, or otherwise affected by venue conditions. No yield is guaranteed.

7.2 Realization and Allocation

Aave-generated yield must be realized and allocated according to protocol rules. Realized yield may be routed through a dispatcher or allocation mechanism. A portion may be allocated to stakers by increasing the amount of S^+ attributable to the staking contract. Other portions may be allocated to protocol fees, treasury functions, security spending, operational reserves, or other disclosed destinations, subject to parameters and governance.

The standard protocol fee on generated yield is expected to be 25%. During disclosed campaigns such as a Farming Season, the protocol fee may be temporarily increased, including up to 50%, if properly disclosed through separate campaign materials. Campaign mechanics, airdrop terms, token distribution, launch valuation, sale terms, or OVER incentives are outside the scope of this Whitepaper.

7.3 Share-Based Accounting

Users who stake S^+ receive sS^+ shares. The exchange rate R determines how much S^+ corresponds to each staking share. When realized yield is allocated to the staking module, R may increase. The base S^+ balance of non-staking holders does not change.

This approach has two consequences:

- Integrators of base S^+ do not need to handle rebasing balances.
- Yield participation is visible as a separate user action and separate token representation.

7.4 Overyield Dynamics

Because yield is allocated only to staking shares, the effective variable yield received by stakers depends on both the yield generated by underlying Aave positions and the proportion of S^+ supply that is staked. If a smaller proportion of S^+ is staked, realized yield is allocated across fewer staking shares. If a larger proportion is staked, realized yield is allocated across more shares.

This dynamic does not create additional system yield, does not guarantee any return, and does not eliminate external venue risk. It is an allocation effect within the protocol's share-accounting design.

7.5 Exchange Rate Limitations

The staking exchange-rate mechanism is designed so that R does not decrease under normal valid accounting transitions. This accounting property should not be interpreted as a guarantee that users cannot suffer economic loss. If Aave, an underlying stablecoin, the protocol, a

cross-chain system, or another dependency is impaired, the nominal exchange-rate variable may not fully reflect practical recoverability, liquidity, market value, or legal enforceability.

7.6 Emergency Withdrawal and Yield Interruption

If the Foundation multisignature wallet triggers emergency withdrawal from Aave, assets may be withdrawn from the external venue and yield generation may stop or decrease. This action may preserve protocol-controlled liquidity under certain conditions, but it does not guarantee that assets can always be withdrawn before a venue event or that all losses can be avoided.

7.7 No Automatic Holder Yield

The protocol should not be described as paying interest, yield, or rewards merely for holding the base overlaid asset. Any protocol-level yield participation requires opt-in staking and a separate staking representation. This distinction is central to the protocol's technical and regulatory-aware design.

8. Cross-Chain Transfer Model

Overlayer is expected to support cross-chain transfer of selected tokens through LayerZero-based omnichain mechanics at launch. Cross-chain functionality increases portability but adds external messaging-layer risk.

8.1 Ethereum as Core Backing Environment

Ethereum is expected to serve as the primary environment for Version 1.0 minting, redemption, and Aave integration. Destination-chain token representations should be understood as cross-chain representations connected to the Ethereum-side backing and accounting model unless otherwise disclosed.

8.2 Omnichain Transfer Mechanics

Where enabled, a cross-chain transfer may use a burn-and-mint or equivalent supply-synchronized mechanism. Tokens transferred from one chain are burned, locked, or otherwise accounted for on the source chain, and corresponding tokens are minted or released on the destination chain according to messages validated by the messaging layer.

Such mechanics are intended to preserve aggregate supply consistency. They do not eliminate messaging risk or configuration risk.

8.3 Messaging-Layer Risk

Cross-chain transfer depends on external infrastructure, including endpoints, relayers, validators, oracles, message libraries, destination-chain execution, and configuration choices.

Failures, delays, misconfigurations, or compromises may affect transfers. In severe cases, cross-chain failure could cause supply or accounting disruption.

Users engaging in cross-chain transfers assume the risk of the relevant messaging layer and destination chain. The protocol does not guarantee that cross-chain transfers will always be available, timely, reversible, or error-free.

8.4 No Independent Destination-Chain Backing

Unless expressly disclosed for a specific deployment, destination-chain representations do not create separate backing reserves on the destination chain. Redemption into underlying stablecoins or receipt tokens remains tied to the relevant core deployment and its supported settlement paths.

9. Planned Auxiliary Module: Reserve Index

The Reserve Index is a planned auxiliary module. It is not part of Version 1.0 core minting, redemption, backing, or staking accounting. Its future deployment, legal treatment, user interface, risk disclosures, and parameters should be documented separately before launch.

9.1 Planned Purpose

The Reserve Index is intended to provide an additional on-chain portfolio and liquidity surface involving Overlaid Assets and other widely used crypto-asset representations. It is not intended to serve as backing for Overlaid Assets, to stabilize their price, to guarantee redemption, or to insure users against losses.

9.2 Planned Composition

The planned Reserve Index composition is expected to use the following target weights unless changed before deployment:

Asset Category	Target Weight
Overlaid Asset	50.00%
WBTC	16.66%
ETH	16.66%
XAUT	16.66%

These weights are not part of Version 1.0 core Overlaid Asset backing and may change before or after deployment subject to the relevant process.

9.3 Risk Isolation

Performance, failure, underperformance, rebalancing losses, asset impairment, or liquidity issues affecting the Reserve Index should not affect the unit backing, minting, redemption, or staking accounting of Overlaid Assets. Reserve Index participants bear the separate risks of the index and its constituents.

9.4 Separate Disclosure Required

Before deployment, the Reserve Index should have separate disclosures covering index composition, rebalancing rules, fees, custody and control, execution venues, circuit breakers, asset selection, tax considerations, legal classification, user interface terms, and risk factors. It should not be marketed as a guaranteed store of value, capital-preservation tool, yield product, or insurance reserve.

10. Security and Risk Considerations

No component of the protocol is risk-free. This section summarizes principal risks and is not exhaustive.

10.1 Smart Contract Risk

Protocol contracts may contain bugs, design errors, implementation errors, integration failures, or unforeseen interactions. Audits, contests, testing, open-source review, and formal processes can reduce but not eliminate smart-contract risk.

The protocol has undergone or is expected to disclose security review by Beosin, Hacken, and a HackenProof contest covering the code intended for deployment. Audit reports should be made public before publication or launch. No audit or contest guarantees security or absence of vulnerabilities.

10.2 Upgrade and Administrative Risk

Upgradeable contracts and Foundation-controlled administrative functions create governance and operational risk. Administrators may make poor decisions, react too slowly, misconfigure parameters, become compromised, or be subject to legal or external pressure. Timelocks and multisignature controls mitigate but do not eliminate these risks.

10.3 Aave Risk

Version 1.0 depends on Aave as the sole external yield venue. Users are exposed to Aave smart-contract risk, governance risk, liquidity risk, utilization risk, oracle or market risk where relevant to Aave, reserve configuration risk, and the risk that aToken positions become impaired or illiquid.

Overlayer does not borrow from Aave and does not recursively leverage positions. This avoids adding protocol-level leverage, but it does not remove the lending-market risks inherited from Aave.

10.4 Underlying Stablecoin Risk

Overlaid Assets inherit risks of the underlying stablecoins they reference. USDC, USDT, or any future supported stablecoin may experience depegging, issuer failure, reserve impairment, transfer restrictions, freezes, policy changes, regulatory action, market loss of confidence, or other events.

The protocol does not guarantee that one unit of a supported stablecoin will equal one unit of fiat value. If USDC or USDT trades below its intended peg, the corresponding overlaid asset remains exposed to that market and issuer risk.

10.5 Receipt-Token Risk

Receipt-token settlement may provide an additional path for minting or redemption, but receipt tokens carry external venue risk. The receipt token may be affected by Aave liquidity, market demand, transferability, secondary market price, or venue-specific restrictions.

10.6 Liquidity and Redemption Risk

Users may be unable to redeem the desired amount at the desired time or into the desired settlement form. Liquidity conditions, Aave utilization, per-block limits, emergency controls, stablecoin issuer actions, blockchain congestion, cross-chain failures, or market stress may delay, limit, or alter settlement.

10.7 Cross-Chain Risk

Cross-chain transfer depends on LayerZero or another disclosed messaging layer. Failures, exploits, misconfigurations, message delays, endpoint failures, destination-chain issues, or governance actions affecting the messaging layer may impair transfers or, in severe cases, affect supply consistency.

10.8 Blacklist and Access Risk

Blacklist functionality exists but is disabled at launch. If activated after the required delay, affected wallets may be blocked from interacting with Overlaid Assets. Hosted interfaces may also restrict access through terms of use, sanctions screening, jurisdictional controls, or wallet screening.

10.9 Regulatory Risk

Regulatory frameworks may change or be interpreted in ways that affect the protocol, Foundation, interface operators, users, integrators, external venues, OVER, staking shares, token sales, airdrops, or future modules. The protocol's design posture does not guarantee favorable treatment.

10.10 Market and Integration Risk

Overlaid Assets may trade above or below the value implied by protocol accounting. Secondary markets may be illiquid or volatile. Integrators may price or treat Overlaid Assets differently. Use as collateral, liquidity, or settlement assets in third-party protocols introduces third-party risk.

11. Governance and the OVER Token

Governance is expected to evolve over time. Version 1.0 begins with a Foundation-controlled phase. OVER is expected to be introduced later and is not required for the core protocol to mint, redeem, stake, unstake, or account for Overlaid Assets.

11.1 Launch Phase

During the launch phase, the Foundation multisignature wallet is expected to control specified administrative functions. These controls are disclosed in Section 5. The launch phase should be understood as an operational and governance transition period rather than a fully decentralized end state.

11.2 Future Governance

Future governance may coordinate protocol upgrades, parameter changes, external venue additions, fee parameters, supported asset decisions, optional module deployment, and ecosystem programs. Such governance may introduce risks, including voter apathy, concentration, capture, conflicts of interest, parameter mismanagement, or regulatory obligations.

11.3 OVER Token Role

If introduced, OVER is intended to facilitate governance coordination. OVER does not represent ownership of the protocol, equity in any entity, debt, a deposit, a right to revenues, a right to reserves, a right to redemption, or a guarantee of economic value. Holding OVER is not required for ordinary minting or redemption of Overlaid Assets.

This Whitepaper intentionally excludes OVER token distribution, sale terms, airdrop design, points programs, FDV assumptions, buyback mechanics, burn mechanics, or valuation narratives.

12. Conclusion

Overlayer defines a smart-contract architecture for wrapping supported stablecoins into non-rebasing overlaid assets while separating settlement functionality from optional yield participation. The base asset is designed for transfer and composability. Yield participation is opt-in and represented by a separate staking share.

The protocol's strength is not that it eliminates risk. It does not. It inherits risk from supported stablecoins, Aave, Ethereum, LayerZero, administrative controls, interfaces, market conditions, and applicable law. Its design goal is to make those risks and assumptions explicit while avoiding additional protocol-level leverage, automatic yield on base settlement balances, and opaque off-chain yield strategies.

Version 1.0 should be understood as a launch-stage deployment with Foundation-controlled administrative functions, upgrade delays, disabled but activatable blacklist functionality, Aave dependency, cross-chain messaging dependency, and future governance plans. Users, integrators, and reviewers should assess the protocol based on deployed code, live parameters, audit reports, legal disclosures, and their own risk tolerance.

Overlayer is therefore best described as a regulatory-aware, non-custodial smart-contract infrastructure protocol for stablecoin overlays, not as a risk-free stablecoin issuer, deposit product, guaranteed-yield product, or legally pre-classified safe harbor asset.

Glossary

Aave The external on-chain lending protocol expected to serve as the sole yield venue for Version 1.0.

Aggregate Unit Backing The protocol's accounting of backing measured in units of a supported underlying asset or supported receipt-token representation, not in guaranteed fiat value.

Blacklist Functionality A disabled-at-launch control module that, if activated after the applicable delay, may allow authorized roles to block specified wallets from interacting with Overlaid Assets.

Emergency Withdrawal A Foundation-controlled function intended to withdraw assets from Aave during elevated venue-risk conditions. It may reduce or halt yield.

Foundation The launch-stage governance or administrative vehicle expected to control specified functions through a multisignature wallet.

Overlaid Asset (S^+) A non-rebasing ERC-20-compatible token minted by the protocol against a supported underlying stablecoin or receipt-token representation.

Receipt-Token Representation (aS) A supported representation of an underlying asset issued by or associated with an external venue, such as an Aave aToken.

Reserve Index A planned auxiliary module expected to include Overlaid Assets, WBTC, ETH, and XAUT at target weights. It is not part of Version 1.0 core backing or redemption.

Staked Representation (sS^+) A share-based staking token representing opt-in participation in protocol yield allocation.

Underlying Stablecoin (S) A supported stable-valued token accepted by a deployment. Version 1.0 is expected to support USDC and USDT.

Version 1.0 The intended initial deployment scope described in this Whitepaper, subject to final deployed code and official deployment notices.

A. Mathematical Appendix: Share Accounting

This appendix describes the intended share-accounting model for staking. It abstracts away implementation details, rounding, fees, emergency states, and external venue impairment unless expressly stated.

A.1 Definitions

At accounting event t:

- T_t^+ denotes total S^+ supply.
- $T_{s,t}^+$ denotes total sS^+ share supply.
- $S_{\text{staked},t}^+$ denotes the amount of S^+ attributable to the staking module.
- R_t denotes the exchange rate between sS^+ and S^+.
- Y_t denotes realized yield available for allocation.

A.2 Exchange Rate

The exchange rate is defined as:

$$R_t = \frac{S_{\text{staked},t}^+}{T_{s,t}^+} \tag{1}$$

where $T_{s,t}^+ > 0$. If no staking shares exist, the initial exchange-rate convention is defined by the deployment parameters.

A.3 Staking

When a user stakes x units of S^+ at time t, the number of shares minted is:

$$\Delta sS^+ = \frac{x}{R_t} \tag{2}$$

Ignoring rounding, staking increases both $S_{\text{staked},t}^+$ and $T_{s,t}^+$ proportionally and does not change R_t.

A.4 Unstaking

When a user redeems y shares of sS^+ at time t, the amount of S^+ returned is:

$$\Delta S^+ = y \cdot R_t \tag{3}$$

Ignoring rounding, unstaking decreases both $S_{\text{staked},t}^+$ and $T_{s,t}^+$ proportionally and does not change R_t.

A.5 Yield Allocation

At an allocation event, realized yield Y_t may be converted or accounted for as an additional amount of S^+ attributable to the staking module:

$$\Delta S^+_{\text{yield},t} = f(Y_t) \tag{4}$$

where f is a deployment-specific allocation function reflecting fees, allocation rates, and protocol rules.

The post-allocation exchange rate is:

$$R_{t+1} = \frac{S^+_{\text{staked},t} + \Delta S^+_{\text{yield},t}}{T^+_{s,t}} \tag{5}$$

assuming no simultaneous staking or unstaking event and $T^+_{s,t} > 0$.

A.6 Normal-State Accounting Properties

Under normal operation and absent implementation errors, venue impairment, emergency accounting changes, or other exceptional states:

- staking and unstaking do not change R except for rounding effects;
- realized yield allocation may increase R;
- holding unstaked S^+ does not increase a user's balance;
- yield participation is isolated in sS^+ share accounting.

These properties do not guarantee fiat value, liquidity, external venue solvency, or absence of loss.

B. Parameter Summary

This appendix summarizes protocol parameters referenced throughout the document. Values are illustrative and may vary across deployments. Parameter changes do not alter core accounting or redemption invariants unless explicitly stated.

B.1 Core Parameters

- **Underlying Asset (S)**: Asset accepted as collateral by a given `OverlayerWrap` deployment.
- **Overlaid Asset (S^+)**: ERC-20 token minted against S at a deterministic ratio.
- **Staking Share (sS^+)**: Share-based representation of staked overlaid assets.
- **Exchange Rate (R)**: Ratio between S^+ attributable to staking and total sS^+ supply.

B.2 Minting and Redemption Parameters

- **Mint Ratio**: Deterministic ratio between supplied S and minted S^+ (typically 1:1).
- **Redemption Ratio**: Deterministic accounting ratio between burned S^+ and the corresponding redemption amount. Settlement may occur in the supported underlying asset or, where enabled, a supported receipt-token representation.
- **Per-Block Mint Limit**: Maximum aggregate amount of S^+ that can be minted in a single block.
- **Per-Block Redeem Limit**: Maximum aggregate amount of S^+ that can be redeemed in a block.

B.3 Yield and Allocation Parameters

- **Yield Allocation Frequency**: Discrete intervals at which realized yield is allocated to staking.
- **Protocol Fee Rate**: Portion of realized yield retained by the protocol.
- **Staker Allocation Rate**: Portion of realized yield converted into S^+ and allocated to staking.

B.4 Governance Parameters

- **Governance Scope**: Set of parameters subject to governance processes.
- **Proposal Thresholds**: Conditions required to submit governance proposals.
- **Voting Period**: Duration of governance voting windows.

B.5 Interoperability Parameters

- **Supported Chains**: Set of chains, if any, on which cross-chain modules are activated for a given deployment.
- **Messaging Layer**: External infrastructure used for omnichain transfers.
- **Transfer Limits**: Constraints applied to cross-chain transfers, if any.

B.6 Parameter Mutability

Parameters may be static or adjustable depending on deployment configuration. Adjustments to parameters do not affect the validity of overlaid assets or the protocol's core accounting invariants unless explicitly stated.

References

[1] **Tether.** "Tether: Fiat currencies on the Bitcoin blockchain." Available at: https://tether.to/en/whitepaper/

[2] **Circle.** "USDC: Digital dollars." Available at: https://www.circle.com/usdc

[3] **Aave.** "Aave V3 Tokenization." Available at: https://aave.com/docs/developers/smart-contracts/tokenization

[4] **Ethereum Improvement Proposals.** "ERC-4626: Tokenized Vaults." Available at: https://eips.ethereum.org/EIPS/eip-4626

[5] **LayerZero.** "Omnichain Fungible Token Standard." Available at: https://docs.layerzero.network/