Vaulto Protocol

A Tokenization Layer for Polymarket-Implied Private Company Valuations

---

Whitepaper

Version 0.1 (Draft)

Vaulto Labs

May 2026

This document describes a commodity-wrapper token referencing CFTC-jurisdictional event contracts traded on Polymarket. It is informational only and does not constitute investment, legal, or tax advice. Refer to Section 2 for legal notices and Section 13 for the full regulatory analysis under which Vaulto Protocol operates.

Abstract

Vaulto Protocol introduces `vCOMPANY_L` and `vCOMPANY_S`, two ERC-20 tokens that wrap a basket of Polymarket Conditional Token Framework (CTF) outcome positions and represent long and short economic exposure to the implied valuation of a private company. The underlying CTF positions are binary event contracts within the subject-matter jurisdiction of the U.S. Commodity Futures Trading Commission, traded on Polymarket — which, following its July 2025 acquisition of QCEX and the CFTC's November 2025 Amended Order of Designation, operates a CFTC-licensed Designated Contract Market and is reopening to U.S. participants. Consistent with the doctrine that a 1:1 wrapper of a commodity is itself a commodity (cf. PAXG, XAUT), the vToken is offered as a commodity-derivative wrapper and is not a security. Users mint vTokens by depositing native USDC; the protocol acquires the corresponding CTF basket through Polymarket V2 and issues vTokens at the live net asset value (NAV) of that basket, less a ten basis point fee. Users redeem at any time by burning vTokens for native USDC at NAV, or by exercising a permissionless on-chain ragequit to claim the pro-rata underlying CTF tokens directly — providing actual delivery of the underlying commodity at the holder's election.

Vaulto pools spread cost at the protocol level rather than charging each user the full Polymarket bid-ask on every trade, and lays the groundwork for a protocol-seeded Uniswap V3 secondary market that targets tight retail-sized spreads anchored to NAV. The pilot product, launching on Polygon mainnet, supports a single market: `vANTHROPIC_L` and `vANTHROPIC_S`, referencing Polymarket's "Anthropic IPO Closing Market Cap" event.

This document specifies the product, the underlying basket construction, the on-chain architecture, the price oracle and risk-containment mechanisms, the mathematical invariants the protocol must preserve, and the legal posture under which Vaulto operates. It is intended for sophisticated users, ecosystem partners, and researchers evaluating the protocol prior to use.

Contents

1 Legal Disclaimer

This whitepaper is provided for informational purposes only. It does not constitute, and shall not be construed as, an offer or solicitation to buy or sell any security, derivative, or other financial instrument in any jurisdiction. Nothing herein is investment, legal, tax, regulatory, or accounting advice. Readers should consult their own advisors before engaging with the Vaulto Protocol.

Commodity-derivative wrapper; not a security. The Vaulto Protocol's `vCOMPANY_L` and `vCOMPANY_S` tokens (the "vTokens") are designed and offered as commodity-derivative wrappers of binary event contracts that fall within the subject-matter jurisdiction of the U.S. Commodity Futures Trading Commission ("CFTC") under the Commodity Exchange Act ("CEA").[1] They are not offered as securities and are not intended to be characterized as such. The vTokens are not registered under the U.S. Securities Act of 1933, and no such registration is sought. Section 12 (Regulatory Posture) sets out the legal analysis on which the protocol relies in full.

Availability and jurisdictional considerations. The vTokens are offered to participants in jurisdictions where the offer and the underlying activity are permitted under applicable local law. In the United States, the protocol's analysis (Section 12) is that vTokens are commodity-derivative wrappers of CFTC-jurisdictional event contracts traded on a venue (Polymarket) that operates a CFTC-licensed Designated Contract Market through its July 2025 acquisition of QCEX[2] and its CFTC-approved Amended Order of Designation of November 25, 2025.[3] The protocol's structural commitment to permissionless on-chain ragequit (Section 5.4) is intended to satisfy the policy intent of the "actual delivery" requirement under CEA §2(c)(2)(D) for retail commodity transactions in a digital-asset context. Users in any jurisdiction remain responsible for their own compliance with local sanctions, anti-money-laundering, taxation, and consumer-protection law.

Underlying instrument character. The underlying Polymarket Conditional Token Framework ("CTF") outcome tokens are binary event contracts of the kind treated by the CFTC, and by U.S. case law including *KalshiEX LLC v. CFTC* (D.C. Cir. 2024),[4] as commodity-character instruments under CEA §1a(47). The CFTC's November 25, 2025 Amended Order of Designation for Polymarket US (QCX, LLC) and the CFTC's 2024 Event Contracts NPRM (89 Fed. Reg. 48968)[5] both rest on this characterization. Vaulto wraps a basket of these instruments in a 1:1, redeemable, ragequit-exitable ERC-20 representation; consistent with the doctrine that a 1:1 wrapper of a commodity (e.g., PAXG and XAUT for physical gold) is itself a commodity for regulatory purposes, the vToken inherits the commodity-derivative character of its underlying.

No equity, no governance. vTokens do not represent equity, ownership, profit-sharing rights, voting rights, or any other claim against any private company referenced (including Anthropic) or against Vaulto Labs or any of its affiliates. There is no "VLT" governance token or planned governance token issuance associated with this protocol at the time of publication. The absence of a governance token is intentional and is part of the protocol's design to avoid features that would tend to convert a commodity-derivative wrapper into a security under Howey-style analysis.[6]

Forward-looking statements. This document contains forward-looking statements about the development,

[1] Commodity Exchange Act, 7 U.S.C. §§ 1 et seq.

[2] Polymarket Acquires QCEX. *PR Newswire,* July 2025. https://www.prnewswire.com/news-releases/polymarket-acquires-cftc-licensed-exchange-and-clearinghouse-qcex-for-112-million-302509626.html

[3] Polymarket Receives CFTC Approval of Amended Order of Designation. *PR Newswire,* November 2025. https://www.prnewswire.com/news-releases/polymarket-receives-cftc-approval-of-amended-order-of-designation-enabling-intermediated-us-market-access-302625833.html

[4] *KalshiEX LLC v. CFTC,* No. 24-5205 (D.C. Cir. 2024). https://media.cadc.uscourts.gov/opinions/docs/2024/10/24-5205-2077790.pdf

[5] Event Contracts NPRM, 89 Fed. Reg. 48968 (June 2024). https://www.federalregister.gov/documents/2024/06/10/2024-12125/event-contracts

[6] *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946).

deployment, and operation of the Vaulto Protocol. These statements are not guarantees of future performance and are subject to known and unknown risks, including those described in Section 11 (Risk Factors). Actual results may differ materially. The information herein is provided as of the publication date and Vaulto Labs assumes no obligation to update any forward-looking statement.

Total-loss risk. vTokens reference outcome contracts that can settle at zero. A user holding `vCOMPANY_L` may lose 100% of deposited capital if the referenced company does not IPO at the relevant valuation threshold within the contract's resolution window. The same is true of `vCOMPANY_S` in the opposite outcome. See Section 11.

Independent legal counsel. Before transacting in vTokens, users in any jurisdiction should obtain their own independent legal, tax, and regulatory advice. The protocol's characterization of vTokens as commodity-derivative wrappers under U.S. law (Section 12) is a position taken in good faith on the available authorities; it has not been blessed by any regulator and is subject to regulatory or judicial reconsideration. Section 11.7 enumerates the principal counter-arguments and the residual risks under which the protocol operates.

---

2 Introduction

2.1 The price-discovery gap for private companies

Late-stage private companies have become a structurally important asset class. As of 2026, the largest privately held technology companies — Anthropic, OpenAI, SpaceX, Stripe, Databricks among them — collectively command implied valuations approaching three trillion dollars, and several have remained private for more than a decade past the point at which prior generations of comparable companies would have completed an initial public offering. The result is an unusual market structure: the most economically significant venture-stage firms in the world trade rarely, opaquely, and only among accredited or institutional counterparties. Public-market participants cannot express views on the valuation trajectory of these companies; secondary-market transactions in their stock occur at discounts of 20–40% to the most recent primary-round price; and price discovery between funding rounds depends on rumor, leaked tender offers, and the inference of a small population of insiders.

Several markets have attempted to fill this gap. Forge Global and EquityZen operate accredited-investor venues for direct secondary transfers, with substantial frictions and low transparency. Tokenized-equity platforms such as Backed Finance and Dinari offer wrapped public securities but cannot wrap unlisted equity. Synthetic perpetual derivatives on private-company tickers have appeared on offshore venues but lack a credible reference price. Most recently, regulated and unregulated prediction markets have begun to list binary outcome contracts on specific corporate events — most importantly, **the closing market capitalization on the first day of trading** if and when the company eventually IPOs.

These prediction markets generate something the secondary tender market does not: a **continuously updating, publicly observable, dollar-settled probability distribution** over the company's eventual IPO valuation. When read in aggregate across multiple valuation brackets ("less than $100B," "$100–200B," and so on), they imply a probability-weighted expected valuation that is, in effect, a market price for the company today. Vaulto Protocol's thesis is that this implied price is the most credible publicly available signal of private-company value, and that wrapping it in a transferable, composable ERC-20 token makes it useful as a building block for downstream financial primitives — long-short trading, hedging, structured products, and on-chain index construction.

2.2 What Vaulto does

Vaulto does not create new outcome contracts, take counterparty risk against a referenced company, or invent a valuation methodology. It performs a single, narrow function: it **wraps an externally priced basket of Polymarket CTF outcome tokens in a redeemable ERC-20 representation**, and provides the mint, redeem, oracle, and risk-containment infrastructure that makes that wrapper trustworthy.

For the launch market — Anthropic — the protocol holds a vault on Polygon that is permitted to acquire and dispose of Polymarket CTF outcome tokens across the eight valuation bands of the event `anthropic-ipo-closing-market-cap-119`. Users who wish to express a long view on Anthropic's implied IPO valuation mint `vANTHROPIC_L`, which is backed by a weighted basket of YES outcome tokens skewed toward the high-valuation bands. Users expressing a short view mint `vANTHROPIC_S`, backed by a basket skewed toward the low-valuation and "no IPO" bands. Both tokens trade continuously, settle to the same underlying CTF positions, and can be exited at any time through three independent paths: (i) primary redemption at NAV through the Vaulto backend, (ii) secondary swap against a protocol-seeded Uniswap V3 pool (planned for protocol version 2), and (iii) on-chain ragequit, which burns the user's vTokens in exchange for the pro-rata underlying CTF tokens with no operator involvement.

2.3 Why a tokenized wrapper

The Polymarket CTF outcome tokens that underlie vTokens are already on-chain ERC-1155 positions. A natural question is why the wrapper is necessary at all. Three reasons motivate the design.

First, **spread amortization**. A user who buys exposure to an eight-band Anthropic event by purchasing each YES outcome separately pays the full Polymarket bid-ask on every band — frequently three to five percent of notional, sometimes more. The protocol absorbs this cost once, at the basket level, and amortizes it across all mints and redeems within a rebalance window. The marginal cost of expressing a view through the wrapper is far lower than the marginal cost of constructing the same basket directly.

Second, **composability**. ERC-1155 positions are not first-class citizens of the on-chain DeFi ecosystem. They cannot be used as collateral in most lending markets, cannot trade in Uniswap V3, and cannot be wrapped by money-market protocols. An ERC-20 with a transparent and on-chain-verifiable backing relationship can serve as the underlying for a much wider class of secondary infrastructure.

Third, **rebalance and roll mechanics**. The Anthropic IPO market resolves on a specific date. The basket's weights must shift over time as the event approaches resolution and as new information narrows the valuation distribution. Maintaining these weights at the level of the individual user — across hundreds of users, eight bands, and an event that may not resolve for months or years — is an unworkable user experience. Maintaining them at the protocol level, with users holding a fungible token, is straightforward.

2.4 Document scope

The remainder of this document specifies the protocol in detail. Section 3 describes the vToken contract surface. Section 4 specifies how the underlying basket is constructed from Polymarket V2 outcome tokens. Section 5 describes the mint and redeem mechanics. Section 6 describes the NAV oracle. Sections 7 through 9 describe the smart-contract architecture, the off-chain operations stack, and the planned Uniswap V3 secondary market. Section 10 is a mathematical appendix. Section 11 enumerates risks. Section 12 sets out the regulatory posture under which Vaulto operates.

---

3 Product Overview: vTokens

This section defines the vToken contract surface, the supply mechanics, the rights conferred on holders, and the fee schedule. Implementation specifics are deferred to Section 7.

3.1 Tokens

For each supported reference event, Vaulto Protocol issues two ERC-20 tokens:

- `vCOMPANY_L` — long token. Backed by a weighted basket of Polymarket CTF YES outcome tokens with weights biased toward higher-valuation bands. The holder of `vCOMPANY_L` profits if the company's eventual IPO closing market cap clears the bands the basket is weighted toward.
- `vCOMPANY_S` — short token. Backed by a weighted basket biased toward lower-valuation bands and the "no IPO by the resolution date" band. The holder of `vCOMPANY_S` profits if the company fails to IPO at the relevant threshold, or fails to IPO at all, within the resolution window.

Both tokens conform to the ERC-20 standard[7] and additionally implement ERC-2612 (`permit`)[8], enabling gasless approvals from supporting frontends. Decimals are fixed at 18, mirroring the convention of the broader Ethereum ecosystem.

The two tokens for a given company share a single underlying vault but reference disjoint subsets of the CTF basket. They are not perpetual: the basket resolves at a specific date determined by the underlying Polymarket event, and the protocol's resolution handling (Section 11.1) governs the lifecycle of the tokens through that resolution.

3.2 Supply mechanics

There is no fixed supply. Tokens are issued on demand and burned on redemption. Total supply at any point in time satisfies the invariant

$$\text{supply}(t) = \sum_{u} \text{balance}(u, t)$$

and the protocol guarantees, by construction and continuous monitoring, that

$$\text{NAV}(t) \cdot \text{supply}_L(t) + \text{NAV}_S(t) \cdot \text{supply}_S(t) \leq \text{TotalAssets}(t)$$

where `TotalAssets` is the value of the vault's holdings denominated in USDC, computed across native USDC, USDC.e, pUSD, and the held CTF basket priced at the oracle's most recent TWAP. The invariant is the subject of an automated reconciler (Section 8) and a Foundry invariant test that exercises the protocol against 128,000 randomized mint, redeem, and ragequit calls.

3.3 Rights conferred

A vToken confers three rights on its holder, exhaustively enumerated:

1. **Redemption at NAV.** The holder may redeem the token through the Vaulto backend at any time prior to event resolution for native USDC, calculated as `burnAmount × NAV / 10^18` less a 10 bps redemption fee. Redemption is subject to the daily redemption cap parameterized per company (initial pilot value:

[7] ERC-20. *EIP-20: Token Standard.* Fabian Vogelsteller, Vitalik Buterin, 2015. https://eips.ethereum.org/EIPS/eip-20

[8] ERC-2612. *EIP-2612: Permit – 712-signed Approvals.* Martin Lundfall et al., 2020. https://eips.ethereum.org/EIPS/eip-2612

$100/day, intended to scale post-audit) and to the availability of vault assets sufficient to cover the redemption.

2. **Ragequit.** The holder may, at any time and without backend involvement, call the on-chain `MintRedeemController.ragequit(...)` function to burn their vTokens in exchange for the pro-rata share of the vault's underlying CTF outcome tokens plus a pro-rata share of the vault's USDC buffer. This right is permissionless, never paused, and survives any operator unavailability. It is the protocol's structural defense against operator-risk concerns; see Sections 5.4 and 12.4.
3. **Secondary trading.** The holder may transfer the token to any other non-U.S. person, subject to ERC-20 transfer mechanics and any future protocol-level transfer restrictions that may be enforced for jurisdictional compliance. In a future protocol version (Section 9), a protocol-seeded Uniswap V3 pool will provide a continuous secondary market against USDC.

vTokens do not confer voting rights, governance rights, dividend rights, or rights against any third party. They do not represent an equity interest in any private company. They do not represent a security interest in Vaulto Labs or any of its affiliates.

3.4 Fee schedule

Action	Fee	Recipient
Mint	10 bps of `usdcIn`	Vaulto Treasury
Redeem	10 bps of `grossUsdc`	Vaulto Treasury
Ragequit	0 bps	—
Secondary swap (v2)	Uniswap V3 pool fee (0.30%)	Liquidity providers

The 10 bps primary fee covers gas, oracle pusher operations, and protocol reserves. The fee schedule is set at the contract level and is subject to a 48-hour timelock for any modification. The maximum allowed fee, enforced in the contract, is 500 bps; the protocol cannot raise fees above this cap without redeploying.

The ragequit path imposes no protocol fee. This is intentional: ragequit is the user's structural exit and must remain economically frictionless to function as the trust-minimizing escape hatch the protocol is designed around.

---

4 Underlying: The Polymarket CTF Basket

This section specifies how Vaulto constructs the basket of Polymarket Conditional Token Framework ("CTF") outcome tokens that backs each vToken. The mechanics described here are not invented by Vaulto; they follow Polymarket's V2 negative-risk event-contract design and exist independent of the wrapper. Vaulto's role is to select which outcome tokens compose the basket, what weights to assign them, and when to rebalance.

4.1 Polymarket V2 negative-risk events[9]

A Polymarket V2 negative-risk ("negRisk") event is a set of mutually exclusive binary outcome contracts whose YES outcomes sum, by construction, to no more than one dollar of payoff per unit of collateral.

[9] Polymarket Conditional Tokens documentation. https://docs.polymarket.com/

For the launch market `anthropic-ipo-closing-market-cap-119`, Polymarket lists eight outcome bands corresponding to disjoint ranges of Anthropic's eventual IPO closing market capitalization:

Band index	Label	Midpoint (USD bn)
0	Less than $100B	50
1	$100B – $200B	150
2	$200B – $300B	250
3	$300B – $400B	350
4	$400B – $600B	500
5	$600B – $900B	750
6	$900B or above	1,200
7	No IPO by resolution date	0

(Exact band boundaries and the resolution date are determined by the Polymarket event specification and may differ from the illustrative table above; the on-chain band token IDs and labels of record are those returned by Polymarket's Gamma API for the canonical event slug.)

Each band has an associated YES outcome ERC-1155 token,[10] traded on Polymarket V2's `NegRiskCtfExchange` on Polygon, settled in pUSD (Polymarket's V2 collateral asset). The price of band *i*'s YES token, denoted $P_i \in [0, 1]$, is the market's instantaneous implied probability that the IPO closing market cap will fall within band *i*. By construction:

$$\sum_{i=0}^{N-1} P_i \leq 1$$

with the residual $1 - \sum P_i$ representing the spread cost (the gap between the sum of bid sides and one dollar).

4.2 Long basket and short basket

For each company, Vaulto defines two baskets, parameterized by two weight vectors $w^L = (w_0^L, \ldots, w_{N-1}^L)$ and $w^S = (w_0^S, \ldots, w_{N-1}^S)$ with $\sum_i w_i^L = \sum_i w_i^S = 1$. The vToken NAV is then

$$\text{NAV}_L = \sum_{i=0}^{N-1} w_i^L \cdot P_i, \qquad \text{NAV}_S = \sum_{i=0}^{N-1} w_i^S \cdot P_i$$

reported in dollars per vToken. Because each $P_i \in [0, 1]$ and weights sum to one, each NAV is bounded in $[0, 1]$. The dollar value of one vToken is therefore at most one dollar, regardless of the company referenced.

The weight vectors are computed using a midpoint-proportional V2 weighting scheme inherited from Vaulto's existing trading infrastructure. Each band i has an associated midpoint m_i (a representative valuation, in dollars, for that band; for the "no IPO" band, $m_7 = 0$). For a long basket targeting a reference valuation level λ^L (chosen by the protocol to bias the basket toward the upper bands), the long weight on band i is

$$w_i^L = \frac{f^L(m_i, \lambda^L)}{\sum_j f^L(m_j, \lambda^L)}$$

[10] ERC-1155. *EIP-1155: Multi Token Standard.* Witek Radomski et al., 2018. https://eips.ethereum.org/EIPS/eip-1155

where f^L is a monotonically increasing kernel that places more weight on bands whose midpoint m_i exceeds λ^L. The short basket uses an analogous decreasing kernel f^S. Exact kernel forms are specified in Section 10. The intuition: a long vToken should profit when prices on the high-valuation bands rise; a short vToken should profit when prices on the low-valuation bands (or the "no IPO" band) rise.

The "no IPO" band is, by convention, weighted into the short basket only. Holders of `vCOMPANY_L` do not benefit from the company failing to IPO; that scenario is the short basket's responsibility.

4.3 Worked example (Anthropic, illustrative)

To make the construction concrete, suppose the eight Anthropic bands have midpoints $(50, 150, 250, 350, 500, 750, 1200, 0)$ billion dollars and the long basket targets $\lambda^L = 500$ billion. A simple midpoint-proportional kernel $f^L(m) = m$ (zero for the "no IPO" band) yields long weights proportional to the midpoints, so

$$\begin{aligned} w^L &= (50, 150, 250, 350, 500, 750, 1200, 0)/3{,}250 \\ &\approx (0.015, 0.046, 0.077, 0.108, 0.154, 0.231, 0.369, 0) \end{aligned}$$

A symmetric short kernel $f^S(m) = m^{-1}$ (with the "no IPO" band assigned a fixed large weight to dominate the bottom of the distribution) produces a vector heavily concentrated on bands 0, 1, and 7. The illustrative values above are not the production weights, which are computed by the V2 pricing module and may incorporate additional path-dependence (the protocol's current expected valuation $\mathbb{E}[m]$ and a midpoint-proportional adjustment factor K; see Section 10). What matters for this section is the property that the two baskets, by construction, span the event's outcome space: long and short are not perfectly negatively correlated, but they are economically meaningful directional bets.

4.4 Basket acquisition and disposition

When a user mints `vCOMPANY_L` with D dollars of USDC, the protocol must, in the steady state, acquire a basket of CTF YES outcome tokens such that:

$$\sum_i (\text{shares acquired in band } i) \cdot P_i \approx D \cdot (1 - \phi_{\text{mint}})$$

where ϕ_{mint} is the mint fee (10 bps in the pilot). The shares purchased in band i are proportional to w_i^L / P_i, so that the dollar value of the holdings is weighted by w^L rather than the share count itself.

Acquisition is performed by the protocol's executor — an off-chain signer authorized via the on-chain `EXECUTOR_ROLE` — submitting Polymarket V2 limit orders with the protocol's `CompanyVault` as the maker. The vault implements ERC-1271 `isValidSignature` and is registered with Polymarket V2 as a `POLY_1271` signer (signature type 3 in Polymarket V2's enum), permitting the executor's EOA signature to authorize fills against the vault's pUSD balance. Order placement, retry, slippage escalation, and fill polling logic are described in Section 8.

Disposition (redeeming a basket back into pUSD, then back into native USDC for distribution to redeeming users) mirrors the acquisition flow. Both directions traverse a fixed sequence of stablecoin hops:

```
Native USDC  ⇌  USDC.e            (Uniswap V3, 0.01% pool)
USDC.e       ⇌  pUSD              (Polymarket Collateral Onramp / Offramp)
pUSD         ⇌  CTF YES tokens    (Polymarket V2 negRisk exchange)
```

The vault holds all four asset types and is pre-approved to the appropriate exchange and adapter contracts. Approval bootstrap is a one-shot `approveCollateralRails(...)` call by the admin role, performed once at vault deployment.

4.5 Rebalance triggers

The protocol rebalances the basket — i.e., adjusts the share counts in each band to maintain the target weights w^L and w^S — under three triggers:

1. **Net mint or redeem flow** that materially changes the basket composition;
2. **Weight drift** in the V2 weight vectors as the protocol's target λ or K parameters update (for instance, as new information narrows the implied valuation distribution);
3. **Event proximity** — as the resolution date approaches and the event distribution sharpens, the protocol may opt to roll into bands more concentrated around the current implied valuation.

Rebalances are operator-initiated; the protocol does not yet provide a public-facing keeper interface for rebalances. The pilot's small TVL ceiling ($100/day mint cap) means that rebalance frequency in the early operating phase will be manageable manually. Future protocol versions are expected to expose a permissionless rebalance interface gated by deviation thresholds.

---

5 Mint and Redeem Mechanics

This section describes the user-facing flows for issuing and burning vTokens. The mechanics are designed for one overriding goal: at every step, either the user retains the right to recover their assets, or the protocol's smart contracts hold the funds under terms the user can verify on-chain.

5.1 The async escrow mint

Polymarket V2 order fills are not atomic with on-chain Polygon transactions. An order can take seconds to minutes to fill, can partial-fill, and can fail to fill at all if the orderbook is thin. A naive mint flow that issued vTokens before the basket was acquired would create unbacked supply. A flow that required the user to wait for fills in real time would force the user to keep an EOA hot for the duration. Vaulto's design is asynchronous: the user funds an escrow, the protocol fills the basket, and the protocol mints once the fill is confirmed.

The full sequence:

1. **Quote.** The user (through the Vaulto frontend) queries the quote endpoint:

   `GET /api/tokens/anthropic/quote?side=LONG&usdcIn=100000000`

   (100 USDC, 6-decimal raw form). The backend reads the on-chain `PriceOracle.nav(companyId, isShort=false)` and returns the live NAV, the expected vToken output, the fee, and a deadline.

2. **Submit.** The user approves the `EscrowVault` for the desired USDC amount (via ERC-2612 permit when supported by the user's wallet, or via a separate `approve` transaction). The user POSTs `/api/trading/mint` with `{companyId: "anthropic", side: "LONG", usdcAmount, slippageBps}`. The backend computes a fresh quote, generates a 32-byte `requestId`, inserts a row in the `tokenization_mint_requests` table with status `PENDING_DEPOSIT`, and calls `EscrowVault.deposit(requestId, user, usdcAmount)` as the holder of `DEPOSITOR_ROLE`. The deposit transfers USDC from the user to the escrow under a per-request accounting tag. The row transitions to status `PENDING_FILL`. The user's frontend receives the `requestId` and begins polling.

3. **Fill.** The backend's `executeMint(requestId)` worker runs. It computes the target band allocation from the current V2 weights, calls `swapAndWrapVault(targetPusd, maxUsdcIn)` to convert the escrowed USDC into pUSD inside the vault (via Uniswap V3 + Polymarket Onramp), and submits Polymarket V2 limit orders for each band, signed under the `POLY_1271` path. The worker polls for fills, tracks `usdcSpent` and `shares acquired per band`, and waits until either (a) the basket is filled to within a minimum fill threshold, or (b) the deadline expires.
4. **Mint.** Once the basket is acquired, the worker reads the current NAV from the oracle and constructs a `MintReceipt` EIP-712 message with the fields `(companyId, isShort, user, usdcIn, mintAmount, navAtFill, nonce, deadline, requestId)`. The receipt is signed by the `MINTER_SIGNER` key, distinct from the executor key. The worker calls `MintRedeemController.mint(receipt, signature)`. The controller validates the signature, the deadline, the nonce (one-time per user), the request ID (one-time per protocol), the NAV deviation against the live oracle (within 200 bps in the pilot), and the daily mint cap. On success, it mints `mintAmount` of `vCOMPANY_L` to the user, debits the 10 bps fee, and emits a `Minted` event.
5. **Confirm.** The worker updates the database row to `FILLED` with the transaction hash. The user's frontend, on its next poll, sees the new status and the user's wallet shows the freshly minted balance.

If fill fails — orderbook too thin, deadline passes, slippage exceeds the user's tolerance — the worker calls `EscrowVault.refund(requestId)` and marks the request `FAILED_LIQUIDITY` or `FAILED_SLIPPAGE`. The user receives their USDC back; no vTokens are minted.

The user therefore has, at every point in the flow: - Funds in their own EOA (before submit), or - Funds in the escrow with a unique, refundable request ID (between submit and fill), or - A backed vToken position (after fill).

There is no intermediate state in which the user has paid USDC but holds neither vTokens nor a refundable claim.

5.2 Redeem (fast path)

Redemption mirrors mint with one structural difference: most redemptions can clear synchronously against the vault's USDC buffer, without going to Polymarket. The flow:

1. The user POSTs `/api/trading/redeem` with `{companyId, side, burnAmount, slippageBps}`.
2. The backend reads the current NAV, computes `grossUsdc = burnAmount × NAV / 10^18`, `netUsdc = grossUsdc × (1 − redeemFeeBps / 10000)`, and verifies `vault.usdcBalance() ≥ grossUsdc`.
3. If the buffer suffices: the backend signs a `RedeemReceipt` and calls `redeem(receipt, sig)` on `MintRedeemController`, which burns the user's vTokens and instructs the vault to push `netUsdc` to the user and `grossUsdc − netUsdc` to the treasury.

Because vault USDC is replenished asynchronously by selling part of the basket on Polymarket when the buffer falls below a target threshold, redemptions in normal operation appear synchronous to the user, with no Polymarket round-trip latency.

5.3 Redeem (slow path)

If the vault's USDC buffer is insufficient for a requested redemption, the slow path engages:

1. The backend executes a sell of the appropriate fraction of the user's pro-rata basket on Polymarket V2 to refill the buffer. This is the inverse of the mint fill, traversing CTF → pUSD → USDC.e → native USDC.
2. Once sufficient native USDC is in the vault, the fast path completes as above.

The slow path adds Polymarket fill latency (seconds to minutes) and is the redemption analog of the mint async flow. The pilot's small TVL ceiling makes the slow path rare; most redemptions in production should land entirely on the buffer.

5.4 Ragequit

The third exit path is structurally distinct from the previous two. It involves no backend, no oracle, no NAV calculation, and no fee. It is permissionless, cannot be paused by the protocol, and is exercisable directly against the smart contracts.

The function signature:

```
function ragequit(bytes32 companyId, uint256 longAmount, uint256 shortAmount) external;
```

A user calling this function from any address with `longAmount` of `vCOMPANY_L` and `shortAmount` of `vCOMPANY_S` in their wallet:

1. Has both balances burned;
2. Receives a pro-rata share of the vault's holdings in each of the long basket's outcome token IDs (in proportion to `longAmount / longSupply`) and each of the short basket's outcome token IDs (in proportion to `shortAmount / shortSupply`);
3. Receives a pro-rata share of the vault's native USDC, USDC.e, and pUSD balances, weighted by the user's combined share of the two supplies.

The user receives the Polymarket CTF outcome tokens as ERC-1155 tokens directly in their EOA. They may then exit those positions through Polymarket's native interface, transfer them, or hold them to resolution.

Ragequit is the protocol's structural answer to operator-risk concerns. If the Vaulto backend goes offline indefinitely; if the executor key is compromised; if the protocol is paused by emergency action; if regulatory action makes the operator unable to honor primary redemptions — none of these conditions affect a user's ability to exit. The on-chain ragequit function depends only on the deployed contracts and the vault's holdings.

It is, equivalently, the protocol's principal defense against the "no actual delivery" prong of the CEA §2(c)(2)(D) retail-commodity rule analysis. A user holding `vCOMPANY_L` is not holding a synthetic claim that the operator promises to settle; they are holding a claim that, at the user's election, becomes the underlying outcome tokens themselves, within a single on-chain transaction. See Section 12 for further discussion.

5.5 Slippage and refund discipline

Both mint and redeem are bounded by a user-set `slippageBps` parameter, defaulting to 100 bps (1%). The backend's signed receipt encodes the actual `mintAmount` (or `usdcOut`) achieved against the live NAV. The on-chain controller refuses to accept a receipt whose `navAtFill` deviates more than 200 bps from the live `nav()` at the time of execution, providing a second, contract-enforced bound. If the achieved fill falls short of the user's tolerance, the request reverts and the user is refunded.

5.6 Daily caps

The pilot enforces a per-company daily mint cap and a per-company daily redeem cap, parameterized at the controller level and subject to admin adjustment. Initial values are $100/day each, intended to allow internal testing without putting meaningful capital at risk during the unaudited phase. The caps reset at UTC midnight.

---

6 NAV and Oracle Design

The Vaulto Protocol depends on an accurate, manipulation-resistant, and freshness-checked NAV signal at several distinct points: the user's quoted mint and redeem rates, the on-chain controller's deviation check against signed receipts, and the off-chain reconciler's solvency invariant. This section specifies the oracle.

6.1 Source: Polymarket CTF mid-prices

The oracle's underlying signal is the mid-price of each band's CTF YES outcome token on Polymarket's V2 orderbook. These prices are publicly observable through Polymarket's Gamma API and are the same prices that drive Polymarket's user-facing UI.

A scheduled job, `oraclePusher`, runs every 60 seconds from a Railway scheduled task hitting a protected endpoint at `/api/cron/tokenization/push-oracle`. The job fetches the current band mid-prices for each pilot company, validates each price is strictly within $(0, 1)$, scales each price to 18 decimals (`priceWad = floor(price × 10^{18})`), and submits a single `pushObservations` transaction to the on-chain `PriceOracle` contract. The transaction is signed by the `ORACLE_PUSHER` key, a dedicated EOA distinct from the executor and minter signer keys.

6.2 On-chain TWAP

The `PriceOracle` contract stores, for each tracked CTF token ID, a ring buffer of up to N recent observations (default $N = 5$). Each observation is a (`priceWad`, `timestamp`) pair. The contract computes a time-weighted average price by taking the arithmetic mean of the buffer's prices, weighted equally. (Equal weighting is justified by the constant inter-push interval; the on-chain code does not need to integrate over irregular intervals.)

The NAV for a company is then

$$\text{NAV}(c, \text{side}) = \frac{\sum_{i \in \text{bands}(c,\text{side})} w_i \cdot \overline{P_i}}{B_{\text{denom}}}$$

scaled to USDC's 6-decimal precision. Here $\overline{P_i}$ is the TWAP price of band i's CTF token, w_i is the band weight (in basis points, $B_{\text{denom}} = 10{,}000$), and bands are the long-side or short-side band set as appropriate.

6.3 Circuit breaker

A per-token-ID circuit breaker fires if a newly pushed observation differs from the most recent prior observation by more than 25%. When tripped, the affected token ID is marked as compromised; any subsequent call to `nav()` that depends on the tripped token reverts with `CircuitBreakerActive`. The protocol pauses mint and redeem until the admin role manually resets the breaker after verifying the price move is consistent with public market data. The 25% threshold is calibrated for the pilot's small basket size and may be tightened in production.

6.4 Staleness

The contract enforces a maximum staleness of 60 seconds in the pilot configuration. A call to `nav()` reverts if any observation in the basket is older than this window. Because the oracle pusher runs every 60 seconds and writes a fresh timestamp on every push, the steady-state observation age is well under the window; the staleness check exists to refuse service if the pusher fails or is censored.

The maximum allowed staleness, set by `setMaxStaleness`, is bounded in the contract to the range $[30, 3600]$ seconds, preventing administrators from disabling the check or making it irrelevantly loose.

6.5 Cross-check against the Vaulto graph oracle

In addition to the on-chain CTF TWAP, Vaulto maintains an existing oracle signer (`VaultoOracle.sol`, deployed in a prior phase) that issues EIP-712 signed snapshots of each company's implied-valuation distribution and a derived fair-value benchmark. The tokenization controller can, optionally, compare the on-chain NAV against the most recent signed Vaulto graph snapshot and refuse to mint or redeem if the two diverge by more than a configurable bound (default 5%). This is a defense-in-depth check, not a primary input; the on-chain CTF TWAP remains the authoritative basis for vault valuation.

6.6 MEV considerations

Because the oracle is updated on a 60-second cadence and a user's mint or redeem reads NAV at the moment the on-chain transaction is mined, there exists a window in which a sophisticated user could anticipate an oracle update and time a mint or redeem to capture the price move. The protocol mitigates this through three mechanisms:

1. The 200 bps NAV-deviation cap in the controller means the backend must re-sign any receipt where the live NAV has moved more than 200 bps from the receipt's `navAtFill`. A receipt that becomes stale is rejected on submission.
2. The TWAP smoother dampens single-observation moves; the on-chain NAV at any point in time is the average of the last five pushes, so a single new push can shift NAV by at most 20% of the gap between the new push and the previous mean.
3. The pilot's small daily cap ($100/day per company) makes any MEV opportunity de minimis in absolute terms. As caps scale, tightening the deviation cap and shortening the staleness window (or moving the oracle to a faster pull-based design) are the appropriate responses.

---

7 Smart Contract Architecture

The on-chain stack consists of seven Solidity contracts deployed on Polygon and organized around three responsibilities: token issuance and burn, asset custody, and price observation. All contracts are written in Solidity 0.8.24 against OpenZeppelin Contracts v5.1[11] and compile with `via_ir` enabled. The suite passes 42 of 42 Foundry tests, including 35 local unit and invariant tests and 7 fork tests against live Polygon mainnet state.

7.1 Contract roster

Contract	Responsibility
`CompanyToken`	The ERC-20 + ERC-20Permit + ERC-20Pausable token. One instance per `(companyId, side)`. Mint and burn restricted to the controller.

[11] OpenZeppelin Contracts v5.1. https://docs.openzeppelin.com/contracts/5.x/

Contract	Responsibility
`TokenFactory`	Deterministic CREATE2 deployer for `CompanyToken`. Predictable token addresses before deploy.
`CompanyVault`	The asset custodian. Holds CTF outcome tokens, native USDC, USDC.e, and pUSD for one company. Implements the executor-gated `executeTrade` and the EIP-1271 `isValidSignature` used by Polymarket V2 POLY_1271 order validation.
`EscrowVault`	Per-request user USDC escrow. Holds deposits between submit and fill. Two roles: `DEPOSITOR_ROLE` (held by the executor key, calls `deposit`) and `CONTROLLER_ROLE` (held by the controller, calls `sweepToVault` and `refund`).
`MintRedeemController`	The central authorization point. EIP-712 receipt verifier, daily-cap enforcer, NAV-deviation gate, signer-rotation timelock, permissionless ragequit entry point.
`PriceOracle`	The on-chain TWAP store. Pushed observations, ring buffer, circuit breaker, staleness checks, weighted NAV computation.
`VaultoAdminTimelock`	An OpenZeppelin `TimelockController` configured with a 48-hour delay for admin actions.

7.2 Role matrix

Role	Held by	Powers
`DEFAULT_ADMIN_ROLE`	Admin multisig (Gnosis Safe)	Grants and revokes all other roles; subject to the 48h timelock for non-emergency actions
`ADMIN_ROLE`	Admin multisig	Configures fees, caps, oracle parameters, band weights; subject to timelock
`PAUSER_ROLE`	Cold pauser EOA (planned: 2-of-3 multisig)	Pauses any contract; no timelock
`CONTROLLER_ROLE` (on `CompanyToken`, `CompanyVault`, `EscrowVault`)	`MintRedeemController`	Issues, burns, moves USDC between escrow and vault, executes ragequit transfers
`EXECUTOR_ROLE` (on `CompanyVault`)	Vaulto executor EOA	Calls `executeTrade` against allowlisted DEX targets and Polymarket V2 contracts
`POLYMARKET_SIGNER_ROLE` (on `CompanyVault`)	Vaulto executor EOA (may be split in future)	EOA whose signatures the vault validates under EIP-1271 for Polymarket V2 order signing
`MINTER_SIGNER` (variable on `MintRedeemController`)	Dedicated EOA, rotatable via 24-hour two-step timelock	EIP-712 signer for `MintReceipt` and `RedeemReceipt`

Role	Held by	Powers
`ORACLE_PUSHER_ROLE` (on `PriceOracle`)	Dedicated EOA	Calls `pushObservations`
`DEPOSITOR_ROLE` (on `EscrowVault`)	Vaulto executor EOA	Calls `deposit` to escrow user USDC

The separation of `MINTER_SIGNER` (off-chain receipt signing) from `EXECUTOR` (on-chain transactions) is deliberate. The minter signer key never touches a transaction; the executor key never signs a mint receipt. A compromise of either reduces the loss surface to the other's domain, and the two can rotate independently. The 24-hour timelock on minter-signer rotation prevents a flash compromise of the admin from instantly swapping the receipt signer.

7.3 Asset custody and approval boundaries

`CompanyVault` holds, per company, four asset classes:

1. Native USDC (the user-facing rail);
2. USDC.e (the transient hop between native USDC and pUSD);
3. pUSD (the Polymarket V2 settlement collateral);
4. CTF outcome tokens across the company's bands (ERC-1155).

Approvals are bootstrapped through a single admin-gated `approveCollateralRails(...)` call, which sets the following allowances (each spender must already be allowlisted via `allowDex`):

- Native USDC → Uniswap V3 SwapRouter02[12] (for USDC ↔ USDC.e swaps).
- USDC.e → Uniswap V3 SwapRouter02 and Polymarket Collateral Onramp.
- pUSD → Polymarket Collateral Offramp, Polymarket CTFExchangeV2, Polymarket NegRiskCtfExchangeV2, Polymarket NegRiskAdapter.
- CTF outcome tokens → `setApprovalForAll` to CTFExchangeV2, NegRiskCtfExchangeV2, and NegRiskAdapter.

The defense-in-depth check `_dex[spender].allowed` in `approveCollateralRails` ensures the admin cannot accidentally grant approvals to a non-allowlisted spender — every spender that receives an approval must have been independently authorized as a target of `executeTrade` first.

7.4 The executor allowlist

The `executeTrade` function on `CompanyVault` is the protocol's single point of contact with external contracts. Its safety depends on three layers:

1. **Address allowlist.** Only addresses pre-authorized by the admin role through `allowDex(address, true, maxUsdcPerCall)` can be called. The set in production is fixed: Uniswap V3 SwapRouter02, Collateral Onramp, Collateral Offramp, CTFExchangeV2, NegRiskCtfExchangeV2, and NegRiskAdapter. No other addresses are reachable from this entry point.
2. **Selector allowlist.** For each allowed address, only specifically authorized function selectors can be called, set via `allowSelector(address, selector, true)`. This is granular: the executor cannot call arbitrary functions on the SwapRouter02 — only `exactInputSingle` and `exactOutputSingle`.
3. **Outflow cap.** Each call passes a `usdcOutCap` parameter. The contract measures the vault's USDC balance before and after the call, and reverts if the net USDC outflow exceeds the cap. This bounds

[12] Uniswap V3 Core. https://uniswap.org/whitepaper-v3.pdf

the blast radius of any executor key compromise to the cap per call (which itself may be further bounded by the per-address `maxUsdcPerCall` set by the admin).

A compromised executor key, in the worst case, can drain up to `min(maxUsdcPerCall, usdcOutCap)` of native USDC per transaction, across an unbounded number of transactions — bounded only by the vault's native USDC balance. Other vault assets (USDC.e, pUSD, CTF tokens) are not subject to this protection and a compromised executor could move them through allowlisted DEX calls. The pilot's small TVL ceiling limits the absolute scale of this risk. Production mitigations include moving the executor key to a Fireblocks or multisig backend, raising the role transfer threshold, and adding a daily aggregate outflow cap.

7.5 EIP-1271 and Polymarket V2 integration[13]

Polymarket V2 defines four signature types for orders submitted to `CTFExchangeV2` and `NegRiskCtfExchangeV2`:

Type	Code	Meaning
`EOA`	0	The signer is an externally owned account
`POLY_PROXY`	1	The signer owns a Polymarket-managed proxy wallet
`POLY_GNOSIS_SAFE`	2	The signer owns a Polymarket-managed Gnosis Safe
`POLY_1271`	3	The maker is a smart contract that implements EIP-1271

`CompanyVault` registers with Polymarket V2 under signature type `POLY_1271`. The vault implements `isValidSignature(bytes32 hash, bytes calldata signature)` using OpenZeppelin's `SignatureChecker.isValidSignatureNow`, returning the magic value `0x1626ba7e` when the recovered address holds `POLYMARKET_SIGNER_ROLE`. The executor's EOA holds this role; the executor signs Polymarket V2 EIP-712 order messages with `maker = vault address` and `signer = executor address`, and Polymarket's exchange calls the vault's `isValidSignature` to authorize the order.

The decision to implement EIP-1271 rather than wrap the vault in a Gnosis Safe was made after confirming Polymarket V2's first-class support for `POLY_1271` ("To be used by smart contract wallets or vaults," per the SDK's typed enum). The EIP-1271 path is gas-lighter, integrates cleanly with the vault's role infrastructure, and supports key rotation through `grantRole` and `revokeRole` calls subject to the standard admin timelock.

7.6 Deployment

The pilot deployment is a single Foundry script (`DeployMainnetPilot.s.sol`) that:

1. Deploys the `VaultoAdminTimelock` with the admin multisig as proposer, executor, and admin;
2. Deploys the `PriceOracle`;
3. Deploys the `EscrowVault`;
4. Deploys the `MintRedeemController` with conservative pilot parameters (10 bps fees, 100 bps NAV deviation, 60 second oracle staleness, 180 second maximum receipt age, $20 minimum mint, $100 daily mint and redeem caps);

[13] ERC-1271. *EIP-1271: Standard Signature Validation Method for Contracts.* Francisco Giordano, Matt Condon, 2018. https://eips.ethereum.org/EIPS/eip-1271

5. Deploys the `TokenFactory`;
6. Deploys the `CompanyVault` for Anthropic with the V2 band weights from the existing pricing infrastructure;
7. Deploys `vANTHROPIC_L` and `vANTHROPIC_S` through the factory;
8. Registers the company on the controller and tightens the pilot parameter set.

Deployment addresses are written to `deployments/137-pilot.json` and consumed by the backend at startup. The post-deploy multisig operations (granting `CONTROLLER_ROLE` on the escrow, granting `POLYMARKET_SIGNER_ROLE` on the vault, allowlisting the six DEX targets, and calling `approveCollateralRails`) are documented in the repository's runbook and gate the protocol's go-live state.

---

8 Off-Chain Operations

The Vaulto backend is the single off-chain component of the protocol. It is operated by Vaulto Labs as a service to users; it does not have custody of user funds (the user's USDC sits in the escrow contract from deposit through fill, and the vault from fill through redeem); it cannot mint tokens without a fresh on-chain signature that the on-chain controller independently verifies; and its unavailability does not impair users' ability to exit the protocol through ragequit.

8.1 Service surfaces

The backend exposes three user-facing endpoint groups, all subject to the existing Vaulto API authentication stack (Privy session tokens plus API-key middleware):

- `GET /api/tokens`, `GET /api/tokens/:companyId/nav`, `GET /api/tokens/:companyId/quote` — read-only queries against the live oracle and the registered token list.
- `POST /api/trading/mint`, `GET /api/trading/mint/:requestId` — request creation and status polling for mint.
- `POST /api/trading/redeem`, `GET /api/trading/redeem/:requestId` — request creation and status polling for redeem.

The backend also exposes two internal cron endpoints, gated by a shared cron secret:

- `POST /api/cron/tokenization/push-oracle` — invoked every 60 seconds; fetches CTF mid-prices and submits a single `pushObservations` transaction.
- `POST /api/cron/tokenization/reconcile` — invoked every 5 minutes; asserts the solvency invariant against on-chain state and retries any mint or redeem request stuck in `PENDING_FILL` for more than 10 minutes.

8.2 Polymarket V2 order execution

The backend signs Polymarket V2 orders with the executor key under the `POLY_1271` signature type, with the company vault as the maker. The signed order payload is submitted to Polymarket's CLOB API endpoint (`clob.polymarket.com/order`) along with the operator's Polymarket L2 API credentials. Fill events are polled through Polymarket's `getOrderStatus` API and reflected into the protocol's `tokenization_oracle_snapshots` and per-request fill tracking tables. The fill-polling, retry, and slippage-escalation logic reuses the existing `placeMarketOrderWithRetry` infrastructure from Vaulto's user-trading pipeline, with the order construction substituted for the vault-maker variant.

8.3 Reconciliation

The reconciler is the protocol's correctness watchdog. Every five minutes it:

1. Reads `vault.totalAssetsUsdc()` from the on-chain vault (the sum of native USDC, USDC.e, pUSD, and CTF holdings at oracle TWAP prices);
2. Reads `vCOMPANY_L.totalSupply()` and `vCOMPANY_S.totalSupply()`;
3. Reads `oracle.nav()` for each side;
4. Computes the outstanding obligations as `Σ supply × nav / 10^18`;
5. Asserts the solvency invariant `totalAssets ≥ obligations`, allowing a 50 bps drift tolerance;
6. Logs to a per-run `reconcile_log` entry and emits an alert to operations if drift exceeds tolerance.

The reconciler also retries any mint or redeem requests stuck in `PENDING_FILL` for more than ten minutes. Stuck requests typically indicate Polymarket orderbook unavailability or a missed fill event; retry safety relies on the on-chain `requestId` being a single-use marker — even an aggressive retry cannot double-mint, because the controller will refuse the second submission.

8.4 Backend isolation

The tokenization backend code is isolated within `src/tokenization/` of the Vaulto API repository and shares only authentication middleware, database connection, and viem client configuration with the existing Vaulto user-trading endpoints. The tokenization signer keys are independent of the existing oracle signer key. The database tables (`tokenization_tokens`, `tokenization_mint_requests`, `tokenization_redeem_requests`, `tokenization_oracle_snapshots`) are independent of the existing trading schema and can be migrated or rolled back without affecting user trading.

---

9 Secondary Market (Protocol v2)

The pilot launches with primary mint and redeem only. A secondary market against Uniswap V3 is planned for protocol version 2, following the pilot's audit and an initial period of operation.

9.1 Design

For each `(companyId, side)` token, the protocol intends to seed a concentrated-liquidity position on Uniswap V3 paired against native USDC at the 0.30% fee tier. The position's liquidity is provided by the protocol from a dedicated treasury allocation, with an initial size of $50,000 per side per company (subject to revision at the time of v2 launch). The position is concentrated in a ±5% range around the current NAV.

The Uniswap V3 LP NFT is held by `CompanyVault` itself. Public liquidity provision is not enabled at v2 launch; the pool is protocol-seeded only. Public LP capacity is a candidate for v3.

9.2 NAV anchoring through arbitrage

Because the primary mint and redeem path settles at NAV (less fees) and the secondary market trades against the protocol's own seeded liquidity, the secondary market price is structurally bounded close to NAV. Specifically:

- If the pool price rises more than 50 bps above NAV, an external arbitrageur can mint at NAV through the primary, sell into the pool, and capture the difference (net of fees).

- If the pool price falls more than 50 bps below NAV, an external arbitrageur can buy from the pool, redeem at NAV through the primary, and capture the difference.

The protocol itself acts as an internal arbitrageur through a 30-second keeper that monitors the deviation and rebalances when economic. Arbitrage profits accrue to the treasury.

9.3 Range management

As NAV drifts, the seeded concentrated-liquidity range may move out of the prevailing pool price. The keeper monitors the relationship and, when NAV moves outside the active range, closes the position and re-opens at a fresh range centered on the new NAV. This is the v2 analog of an LP "rebalance" and is fully on-chain.

9.4 Why not at launch

Three considerations argue for deferring the secondary market past pilot:

1. **Code complexity.** The Uniswap V3 integration adds approximately 800 lines of contract code and a non-trivial keeper job. Both deserve audit attention separate from the core protocol.
2. **Capital efficiency.** Concentrated-liquidity positions can suffer impermanent loss if NAV moves outside the range without an immediate rebalance. The protocol's treasury allocation is finite and the pilot's small cap means there is little user demand to justify the LP commitment.
3. **Audit sequencing.** The pilot's audit scope is intentionally narrow. Adding the AMM defers the audit by weeks and risks a less rigorous review.

The secondary market is a feature, not a primitive. The protocol functions completely without it.

---

10 Mathematical Appendix

This section states the formal definitions and invariants that govern the protocol. Notation and constants are summarized first; then the basket weights, the NAV, the mint and redeem identities, and the ragequit distribution. A worked Anthropic example follows at the end.

10.1 Notation

Symbol	Meaning
N	Number of bands in a company's event (8 for Anthropic)
$i \in \{0, \dots, N-1\}$	Band index
m_i	Midpoint of band i, expressed in USD billions of market cap
$P_i(t)$	TWAP price of band i's CTF YES outcome token at time t, on $[0, 1]$
w_i^L, w_i^S	Long and short basket weights for band i, satisfying $\sum w_i^L = \sum w_i^S = 1$
λ	The protocol's current target valuation level (USD billions)
K	Midpoint-proportional adjustment factor

Symbol	Meaning
ϕ_m, ϕ_r	Mint fee and redeem fee, expressed as fractions (pilot: $\phi_m = \phi_r = 10/10{,}000 = 0.001$)
WAD	10^{18} — vToken decimal base
USDC_d	10^6 — native USDC decimal base

Times are continuous; on-chain prices update on a discrete 60-second cadence.

10.2 Band weights (V2 midpoint-proportional)

The long basket weight on band i is

$$w_i^L = \frac{f^L(m_i; \lambda, K)}{\sum_{j=0}^{N-1} f^L(m_j; \lambda, K)}, \qquad f^L(m; \lambda, K) = \max\!\big(0,\ m - \lambda + K\big)$$

with $f^L = 0$ enforced for the "no IPO" band ($m_7 = 0$ by convention, but the long basket excludes it by setting $w_7^L = 0$). The parameter λ shifts the weighting toward higher-valuation bands; larger K produces a flatter, more diversified weight vector.

The short basket weight on band i is

$$w_i^S = \frac{f^S(m_i; \lambda, K)}{\sum_{j=0}^{N-1} f^S(m_j; \lambda, K)}, \qquad f^S(m; \lambda, K) = \begin{cases} \max\!\big(0,\ \lambda - m + K\big) & i \neq 7 \\ \mu_S & i = 7 \end{cases}$$

where μ_S is a fixed "no IPO" mass parameter that gives the short basket meaningful exposure to the residual band. In the pilot $\mu_S = 0.20$ (re-normalized after the rest of the vector is computed). The choice of λ, K, μ_S is made by the protocol operator and is the subject of admin-gated `setBandConfig` calls, which are themselves subject to the 48-hour timelock.

10.3 NAV

For the long token of company c,

$$\text{NAV}_L(c, t) = \sum_{i=0}^{N-1} w_i^L(c) \cdot \overline{P_i}(t)$$

where $\overline{P_i}(t)$ is the TWAP of band i's CTF price over the on-chain ring buffer at time t. Because $\overline{P_i} \in [0, 1]$ and weights sum to 1, $\text{NAV}_L \in [0, 1]$ — that is, a single vToken is worth at most one dollar of USDC. The short NAV is defined analogously.

The on-chain function `PriceOracle.nav(companyId, isShort)` returns the NAV in USDC base units:

$$\text{nav}_{\text{usdc}} = \big\lfloor \text{NAV} \cdot \text{USDC}_d \big\rfloor.$$

A value of $500{,}000$ corresponds to 0.50 USDC per vToken.

10.4 Mint identities

Let a user mint with D USDC base units (6 decimals) at NAV nav_{usdc}. The on-chain controller computes:

$$g = \lfloor D \cdot \text{WAD} \,/\, \text{nav}_{\text{usdc}} \rfloor$$

(gross mint amount, 18-decimal vTokens), and

$$n = \lfloor g \cdot (1 - \phi_m) \rfloor$$

(net mint amount, 18-decimal vTokens). The controller mints n vTokens to the user. Fee revenue, in USDC base units, is

$$\phi_m \cdot D$$

routed to the treasury immediately after the mint.

The pre-signed receipt's `mintAmount` field is the value of n; the receipt's `navAtFill` is the value of nav_{usdc} at the moment the backend signed; and the controller verifies that the live `nav()` at execution time is within 200 bps of `navAtFill`.

10.5 Redeem identities

For a redemption of b vTokens (18-decimal):

$$g_{\text{usdc}} = \lfloor b \cdot \text{nav}_{\text{usdc}} \,/\, \text{WAD} \rfloor \qquad \text{(gross USDC)}$$

$$n_{\text{usdc}} = \lfloor g_{\text{usdc}} \cdot (1 - \phi_r) \rfloor \qquad \text{(net USDC to user)}$$

Fee revenue is $g_{\text{usdc}} - n_{\text{usdc}}$ routed to treasury.

10.6 Solvency invariant

Let $S_L(t)$ and $S_S(t)$ denote the total supplies of the long and short vTokens at time t, and $A(t)$ the vault's total assets (native USDC + USDC.e + pUSD + CTF basket valued at TWAP) in USDC base units. The protocol's central solvency invariant is

$$\text{NAV}_L(t) \cdot S_L(t) + \text{NAV}_S(t) \cdot S_S(t) \;\le\; A(t) \cdot \text{WAD} \,/\, \text{USDC}_d$$

(with a 50 bps drift tolerance to accommodate rounding accumulation across many small operations). The off-chain reconciler checks this every five minutes; the Foundry invariant test exercises it across 128{,}000 randomized mint, redeem, ragequit, and price-push call sequences.

10.7 Ragequit distribution

For a ragequit burning b_L long tokens and b_S short tokens, with current supplies S_L and S_S:

For each long band i, the user receives

$$\Delta_i^L = \lfloor B_i \cdot b_L \,/\, S_L \rfloor$$

CTF tokens, where B_i is the vault's holding of band i. The short bands' distribution is symmetric.

The user also receives a pro-rata share of the vault's USDC buffer. Let $U(t)$ be the vault's native USDC balance and let the combined share factor be

$$\sigma = \frac{b_L \cdot \text{WAD}}{S_L + S_S} + \frac{b_S \cdot \text{WAD}}{S_L + S_S}$$

then the USDC payout is $\lfloor U \cdot \sigma / \text{WAD} \rfloor$. The vault's USDC.e and pUSD balances are not distributed in ragequit (they are operational rather than user-facing assets); they remain in the vault and represent residual operational capital. This means a ragequiting user receives at most a fractional share of the most easily-denominated asset and the full pro-rata fraction of the user-facing CTF basket. Users who want a clean cash exit should prefer the redeem path; ragequit is for trust-minimized recovery of the underlying.

10.8 Worked example (Anthropic, illustrative)

Suppose, at time t:

- The eight Anthropic CTF mid-prices are $\overline{P} = (0.02, 0.04, 0.06, 0.08, 0.20, 0.20, 0.36, 0.04)$ (so $\sum \overline{P_i} = 1.00$, a degenerate no-spread example for illustration).
- Long weights $w^L = (0.015, 0.046, 0.077, 0.108, 0.154, 0.231, 0.369, 0)$.
- Short weights $w^S = (0.30, 0.20, 0.15, 0.10, 0.05, 0.05, 0, 0.15)$.

Then

$$\text{NAV}_L = 0.015 \cdot 0.02 + 0.046 \cdot 0.04 + \cdots + 0.369 \cdot 0.36 + 0 \cdot 0.04 \approx 0.2335$$

$$\text{NAV}_S = 0.30 \cdot 0.02 + 0.20 \cdot 0.04 + \cdots + 0 \cdot 0.36 + 0.15 \cdot 0.04 \approx 0.0376$$

On-chain `nav` values: $\text{nav}_L = 233{,}500$ and $\text{nav}_S = 37{,}600$.

A user minting `vANTHROPIC_L` with $D = 100{,}000{,}000$ (100 USDC) receives

$$g = \lfloor 100{,}000{,}000 \cdot 10^{18} \,/\, 233{,}500 \rfloor = 428{,}266{,}380{,}856{,}530{,}534$$

gross vTokens, and

$$n = \lfloor g \cdot 9{,}990 \,/\, 10{,}000 \rfloor \approx 4.278 \cdot 10^{17}$$

net vTokens (approximately 0.4278 `vANTHROPIC_L`). Fee revenue is $10^5 = 100{,}000$ USDC base units (0.10 USDC), routed to treasury.

Were the user to redeem all n tokens at the same NAV, gross redemption would be $\lfloor n \cdot 233{,}500 / 10^{18} \rfloor = 99{,}900{,}000$ USDC base units (99.90 USDC), and net would be $\lfloor 99{,}900{,}000 \cdot 9{,}990 / 10{,}000 \rfloor = 99{,}800{,}100$

USDC base units (~99.80 USDC). Total round-trip cost: 20 bps of notional, consistent with the protocol's stated fee schedule.

The same user could instead ragequit their balance, in which case they would receive a pro-rata share of the vault's long-band CTF holdings and a pro-rata share of the native USDC buffer. The total economic value of the ragequit distribution, valued at the TWAP, equals the mint-weighted contribution to the basket (less any prior fee already paid and any operational frictions).

---

11 Risk Factors

A holder of vTokens is exposed to a broad set of risks. The following enumeration is intended to be exhaustive within the protocol's current design; it is not a substitute for the holder's own due diligence. Each numbered subsection identifies a risk category, the specific mechanism through which the risk affects holders, and any structural mitigation that the protocol provides.

11.1 Event resolution and the "no IPO" outcome

vTokens reference an event with a fixed resolution date determined by Polymarket. When the event resolves, the Polymarket CTF outcome tokens settle to either zero or one dollar per share, and the protocol's basket holdings consequently settle to a deterministic final value. From that moment forward, the NAV of each vToken is fixed.

If the referenced company fails to IPO by the event's resolution date, the "no IPO" band's YES token settles to one dollar and all other bands settle to zero. `vCOMPANY_L`, which excludes the "no IPO" band from its basket, becomes worth zero. `vCOMPANY_S`, which includes the "no IPO" band at a meaningful weight, retains value proportional to that weight. Holders of `vCOMPANY_L` in this scenario lose 100% of their position's value.

The symmetric case applies if the company IPOs at a valuation outside the long basket's weighted range: `vCOMPANY_L` may settle far below its mint price even if the company IPOs. The protocol does not guarantee any particular outcome; vTokens are not principal-protected.

Post-resolution, the protocol enters a "resolved" state for the affected company: new mints halt, redemptions continue at the final NAV for a fixed unwind window (initial proposal: 30 days), after which any remaining vToken supply is force-redeemed at the final NAV and the vault is wound down. Any holder who has not redeemed before the unwind window closes can still ragequit to the underlying basket (now settled to zero or one as appropriate).

11.2 Polymarket counterparty risk

The protocol depends on Polymarket continuing to operate. If Polymarket's offshore international platform is shut down by enforcement action, if its smart contracts are paused, if its API becomes unavailable, or if its operator becomes insolvent, the protocol's ability to acquire and dispose of basket positions is impaired. The vault would retain its CTF outcome tokens (those are on-chain assets independent of Polymarket's operator), and users could still ragequit those tokens out of the vault. But primary mint and redeem operations against the protocol would degrade or halt, and the secondary market would price the wrapper accordingly.

This is the principal counterparty risk Vaulto inherits from the underlying. It is, structurally, the same risk that any direct Polymarket user faces; the wrapper does not amplify it but also does not eliminate it. Ragequit

is the structural defense, but ragequit returns CTF tokens that themselves depend on Polymarket's resolution infrastructure.

11.3 CTF illiquidity

Polymarket's orderbook depth on individual band tokens, particularly far-from-market bands, can be thin. A mint or redeem that touches a thin band can incur slippage that consumes the user's slippage budget, causing the request to fail. The protocol's mitigation is the user-set `slippageBps` parameter and the automatic refund on slippage breach; the user is never silently filled at a worse price.

Beyond user-facing slippage, thin liquidity means the vault's basket positions cannot be unwound at NAV in size. A large redemption that exhausts the USDC buffer requires selling CTF tokens to refill; if the orderbook cannot absorb the sale at NAV, the protocol must either accept fill at a worse price (degrading remaining holders' NAV) or refuse to fill (failing the redemption). The pilot's small cap keeps these scenarios infrequent in absolute terms, but the risk persists in any operating regime.

11.4 Oracle manipulation

The NAV is derived from Polymarket CTF mid-prices observed at a 60-second cadence and averaged across a five-observation TWAP. An attacker who can move Polymarket prices, for instance through wash trading or spoofing in a thin band, can move the on-chain NAV in their favor and time a mint or redeem to capture the difference. The protocol's mitigations are:

- The TWAP smoother, which dampens single-observation moves;
- The 25% per-observation circuit breaker, which trips a band entirely if a single push deviates that much from the prior observation;
- The 200 bps NAV-deviation cap in the controller, which prevents the backend's signed receipt from being executed at a stale NAV;
- The 60-second staleness check, which halts mint and redeem if the oracle has not been updated.

These mitigations are layered. They do not eliminate the risk. An attacker with the capital to move Polymarket prices on a sustained basis could still extract value from the wrapper; the wrapper's cost of attack is the same as the cost of moving Polymarket's published mid.

11.5 Smart-contract risk

The protocol's smart contracts have been tested locally (42 of 42 Foundry tests passing, including a 128{,}000-call invariant test) and reviewed internally. They have not, at the time of pilot launch, been audited by an external firm. Smart-contract bugs — reentrancy, integer overflow, access-control misconfiguration, signature replay — could result in loss of vault funds or unauthorized minting. The pilot's $100/day cap bounds the absolute scale of loss that any single bug could produce in a single day. An external audit is gated to precede the cap increase past pilot levels.

OpenZeppelin Contracts v5.1[14] is the protocol's primary external dependency. A bug in OZ's `AccessControl`, `Pausable`, or `ReentrancyGuard` would propagate to Vaulto.

11.6 Off-chain signer compromise

The protocol's backend operates three independent EOAs: the executor (which sends on-chain transactions and signs Polymarket V2 orders), the minter signer (which signs `MintReceipt` and `RedeemReceipt` EIP-712

[14] OpenZeppelin Contracts v5.1. https://docs.openzeppelin.com/contracts/5.x/

messages), and the oracle pusher (which signs `pushObservations` transactions). A compromise of any of these keys creates a specific exposure:

- **Executor key compromise** allows the attacker to call `executeTrade` with arbitrary calldata against the allowlisted DEX targets, bounded by the per-call USDC outflow cap. The attacker can also place Polymarket V2 orders against the vault as maker, potentially at unfavorable prices that drain the vault's pUSD balance.
- **Minter signer compromise** allows the attacker to sign mint or redeem receipts at NAV deviations within the controller's 200 bps band. Combined with knowledge of a user's nonce, the attacker could mint vTokens to themselves up to the daily cap. The 24-hour timelock on signer rotation means an attacker has at most 24 hours of exposure window before the admin can install a fresh signer; for a $100/day cap, that's $2,400 of maximum potential loss before rotation completes.
- **Oracle pusher compromise** allows the attacker to push false CTF prices, triggering the circuit breaker (and halting the protocol) but also potentially fitting within the 25% deviation tolerance to bias NAV in a favorable direction. The 200 bps NAV deviation cap and the 5-observation TWAP limit the per-transaction impact.

The protocol's mitigation is the role separation itself: no single key compromise produces unbounded loss. Production deployments are expected to migrate signing to a Fireblocks-style key management service or a multisig backed by hardware security modules.

11.7 Recharacterization risk (Howey / security-based swap analysis)

The protocol's regulatory thesis (Section 12) is that vTokens are commodity-derivative wrappers of CFTC-jurisdictional event contracts and inherit their underlying's commodity character under the 1:1-wrapper doctrine exemplified by PAXG, XAUT, and other tokenized-commodity precedents. That thesis is taken in good faith and is, in the protocol's view, the better reading of the law on the facts. It is not, however, the only available characterization, and users should understand the principal recharacterization risks:

- **Howey wrapper recharacterization.** A regulator or court could conclude that the wrapper itself constitutes an investment contract under *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946),[15] notwithstanding the commodity character of the underlying. The strongest factual hooks are (i) the pooled basket structure (horizontal commonality across holders), (ii) the operator's role in band selection, weight setting, oracle operation, and trade execution ("efforts of others"), and (iii) the economic exposure to a specific identified issuer's eventual IPO valuation. The SEC's March 2026 wrapping guidance acknowledges that wrappers are analyzed on their own facts;[16] *SEC v. Terraform Labs* (2024)[17] found that synthetic tokens referencing equity-like values constituted unregistered security-based swaps. The protocol's structural defenses against this argument are the absence of any governance token or protocol-equity instrument, the permissionless ragequit that makes the wrapper a unit-of-account abstraction over directly-owned underlying, and the operator's open commitment to migrate toward permissionless rebalancing and minting.
- **Security-based swap recharacterization.** A regulator could conclude that the vToken's economic terms make it a security-based swap under Securities Exchange Act §3(a)(68)[18] because the payoff references the value of a single private issuer's equity. The protocol's response is that the underlying instrument is a binary event contract (a swap under CEA §1a(47), within CFTC jurisdiction), not a

[15] *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946).

[16] SEC Chair Paul S. Atkins, "Project Crypto" (November 2025). https://www.sec.gov/newsroom/speeches-statements/atkins-111225-secs-approach-digital-assets-inside-project-crypto

[17] *SEC v. Terraform Labs,* No. 23-cv-1346 (S.D.N.Y. 2024).

[18] Securities Exchange Act of 1934, §3(a)(68) (security-based swap definition).

continuous-value referenced security, and that the wrapper's payoff is therefore a function of CFTC-jurisdictional event-contract prices rather than of any security price directly.

- **Retail commodity rule (CEA §2(c)(2)(D)).** Even within a commodity characterization, certain retail leveraged or financed commodity transactions are restricted unless "actual delivery" occurs within 28 days. The protocol's permissionless ragequit (Section 5.4) provides on-chain actual delivery of the underlying CTF outcome tokens at the holder's election, with no operator role or settlement delay. This is the protocol's structural response; it is not a substitute for any specific regulatory clearance.

The residual risk under each of these is real. A regulator could initiate an enforcement action, a court could issue an unfavorable ruling, or the underlying authorities could shift. In any such case, the protocol's response would be to engage transparently, adapt the structure if and as required, and rely on the ragequit path to ensure that holders retain a clean exit to the underlying.

11.8 Operator and protocol availability

The protocol depends on the continued operation of the Vaulto backend service for primary mint and redeem. If the operator becomes unavailable (insolvency, regulatory action, voluntary cessation of operations), users lose access to primary redemption at NAV. The ragequit path continues to function — it has no operator dependency — but it returns underlying CTF tokens rather than USDC, and those tokens themselves depend on Polymarket. A user holding vTokens at the moment of operator unavailability has two exits: ragequit to CTF, or (if available) secondary market sale to another holder.

11.9 Network and infrastructure risks

The protocol operates on Polygon. A Polygon chain halt, validator slashing event, sequencer compromise, or other base-layer failure would impair the protocol. Polygon's reorg history and current sequencer model are inherited risks; we do not undertake to enumerate them here but refer users to Polygon's own documentation.

The protocol depends on the underlying tokens (native USDC, USDC.e, pUSD) maintaining their pegs. A meaningful depeg of any of the three would propagate into the vault's accounting and NAV.

11.10 Geopolitical, sanctions, and enforcement risk

The protocol applies KYC and sanctions screening at the frontend across all jurisdictions and excludes participants located in countries subject to comprehensive U.S. or allied sanctions (notably including Cuba, Iran, North Korea, Syria, the Crimea region of Ukraine, and the Donetsk and Luhansk regions). The protocol may, at the operator's discretion or in response to legal compulsion, block specific addresses or jurisdictions from frontend access. Such blocks do not affect a holder's on-chain ability to transfer, redeem (subject to any compliance constraint at the redemption endpoint), or ragequit (which is permissionless and not gated by the frontend).

Enforcement risk inheres in the protocol's regulatory posture (Section 12). The position that vTokens are commodity-derivative wrappers and not securities is taken in good faith; a U.S. regulator could disagree. The protocol commits to good-faith engagement with U.S. and non-U.S. regulators, to transparent operations including this whitepaper and on-chain reconciliation, and to adapting the structure if and as regulatory expectations clarify. None of these commitments insulates holders from the possibility that the operator could be required to suspend service, restrict access, or change the protocol's terms in response to enforcement action.

11.11 Total-loss disclosure

A holder of vTokens may lose 100% of the value deposited. The combination of event-resolution risk (12.1), Polymarket counterparty risk (12.2), and oracle manipulation (12.4) creates pathways through which the wrapper could become worthless. Holders should treat any allocation to vTokens as risk capital and size positions accordingly.

---

12 Regulatory Posture

This section sets out the legal framework within which Vaulto Protocol operates. The protocol takes the position that vTokens are commodity-derivative wrappers of CFTC-jurisdictional event contracts and that, on the better reading of the applicable authorities, they are not securities under U.S. federal law. The argument proceeds in four steps: (i) the underlying instruments are commodity interests under the Commodity Exchange Act; (ii) Polymarket, the venue on which the underlying is listed, operates a CFTC-licensed Designated Contract Market and is opening to U.S. participants under CFTC oversight; (iii) a 1:1 wrapper of a commodity is itself a commodity under the doctrine consistently applied to tokenized-commodity products such as PAXG and XAUT; and (iv) the protocol's permissionless on-chain ragequit satisfies the policy intent of any "actual delivery" requirement that would otherwise constrain offerings to retail commodity participants. Each step is set out below, followed by the principal counter-arguments and how the protocol responds to them. As Section 1 (Legal Disclaimer) makes clear, nothing in this section is legal advice; holders should obtain their own counsel.

12.1 The underlying instruments are commodity interests under the CEA

The Polymarket CTF outcome tokens that compose the vToken basket are binary outcome contracts that settle on the basis of a publicly observable real-world event — in the launch market, Anthropic's closing market capitalization on its first day of public trading (or the absence of such trading by a specified date). Under the Commodity Exchange Act,[19] instruments of this character — a payoff conditioned on the occurrence or non-occurrence of a specified event — fall squarely within the statutory definition of "swap" at §1a(47), which encompasses any agreement that "provides for any purchase, sale, payment, or delivery … that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence."

The CFTC has consistently treated event contracts of this character as falling within its subject-matter jurisdiction. The agency's 2024 Event Contracts NPRM (89 Fed. Reg. 48968)[20] reaffirmed that binary event contracts of this kind are swaps within Title VII of the Dodd-Frank Act. The D.C. Circuit's October 2024 decision in *KalshiEX LLC v. CFTC* (No. 24-5205)[21] confirmed the lawful scope of CFTC-licensed listings of such event contracts. The CFTC voluntarily dismissed its appeal in May 2025, leaving the D.C. Circuit's analysis undisturbed.

The CFTC itself has applied this characterization directly to Polymarket. In 2022, the CFTC entered into a $1.4 million settlement with Blockratize, Inc., the operator of Polymarket,[22] for offering off-exchange

[19] Commodity Exchange Act, 7 U.S.C. §§ 1 et seq.

[20] Event Contracts NPRM, 89 Fed. Reg. 48968 (June 2024). https://www.federalregister.gov/documents/2024/06/10/2024-12125/event-contracts

[21] *KalshiEX LLC v. CFTC,* No. 24-5205 (D.C. Cir. 2024). https://media.cadc.uscourts.gov/opinions/docs/2024/10/24-5205-2077790.pdf

[22] CFTC Order on Blockratize (Polymarket). PR 8478-22, 2022. https://www.cftc.gov/PressRoom/PressReleases/8478-22

event-based binary options — the same kind of CTF outcome tokens that today underlie vTokens. The settlement order is the agency's own contemporaneous statement that these instruments are CFTC-jurisdictional commodity interests.

12.2 The venue is opening to U.S. participation under CFTC oversight

In July 2025, Polymarket completed its $112 million acquisition of QCEX[23], a CFTC-licensed Designated Contract Market (DCM) and Derivatives Clearing Organization (DCO). QCEX now operates as QCX, LLC d/b/a "Polymarket US." On November 25, 2025, the CFTC issued an Amended Order of Designation[24] formally recognizing Polymarket as an intermediated trading platform operating under QCEX's DCM and DCO licenses; Polymarket relaunched for U.S. participants beginning December 2, 2025, with the prior U.S. waitlist dissolved through 2026. Polymarket-listed event contracts on the U.S. venue are CFTC-regulated commodity derivatives under direct agency oversight.

Polymarket's U.S. relaunch reflects a deliberate strategic and regulatory transition. The protocol's expectation, supported by Polymarket's public communications and the trajectory of its CFTC filings, is that the full breadth of event-contract categories — including company-specific IPO valuation bands — will progressively be available under U.S. DCM listing. As that progression continues, the vault's holdings sit squarely within the CFTC's regulatory perimeter, and the legal character of the wrapper is unambiguously commodity-derivative.

To the extent that, at any particular moment, a specific Polymarket event has not yet migrated to the U.S. DCM listing surface and trades only on Polymarket's international platform, the CFTC's subject-matter jurisdiction over off-exchange swaps under CEA §2(a)(1)(A) — the same jurisdictional theory under which the agency settled with Blockratize in 2022 — continues to apply. The instrument is a commodity interest regardless of the venue's registration status; only the agency's enforcement posture changes between regulated and unregulated venues.

12.3 A 1:1 wrapper of a commodity is itself a commodity

The vToken is a 1:1, redeemable wrapper. Each unit of supply is backed, by on-chain construction and continuously verifiable through the protocol's reconciler, by a corresponding pro-rata claim on the underlying CTF basket. The wrapper has no synthetic exposure, no embedded leverage, no derivative payoff distinct from the underlying, and no unbacked supply.

The legal characterization of such a wrapper follows the doctrine consistently applied to tokenized commodity products. Paxos Gold (PAXG) wraps physical gold held at a custodian and is treated as a commodity interest with no securities-law overlay; Tether Gold (XAUT) operates analogously. Synthetix's sXAU and similar oracle-priced commodity synthetics have likewise been analyzed as commodity-character instruments, not securities. The U.S. Securities and Exchange Commission has not, to the protocol's knowledge, brought an enforcement action against the issuer of a 1:1 commodity wrapper for the unregistered offer and sale of securities. The SEC's March 2026 wrapping guidance is explicit that wrapping a non-security does not convert it into a security and that wrappers are analyzed on their own facts; the relevant facts here — 1:1 backing, redeemability, transparent reserve composition, no embedded leverage — track the PAXG-style precedent rather than the synthetic-equity recharacterization fact pattern in *SEC v. Terraform Labs* (2024)[25]

[23] Polymarket Acquires QCEX. *PR Newswire,* July 2025. https://www.prnewswire.com/news-releases/polymarket-acquires-cftc-licensed-exchange-and-clearinghouse-qcex-for-112-million-302509626.html

[24] Polymarket Receives CFTC Approval of Amended Order of Designation. *PR Newswire,* November 2025. https://www.prnewswire.com/news-releases/polymarket-receives-cftc-approval-of-amended-order-of-designation-enabling-intermediated-us-market-access-302625833.html

[25] *SEC v. Terraform Labs,* No. 23-cv-1346 (S.D.N.Y. 2024).

or the SEC's Mirror Protocol guidance.

The vToken's specific features that arguably introduce wrapper-level complexity — the band-basket composition, the protocol's role in selecting weights, and the 10 basis-point mint and redeem fees — are characteristic of commodity-index products generally and do not, in the protocol's view, alter the underlying analysis. A commodity-index wrapper that holds a basket of CFTC-jurisdictional instruments and prices itself at the basket's verifiable NAV is, on the better reading, a commodity-derivative wrapper. The principal counter-arguments to this characterization are addressed in §13.5 below.

12.4 Ragequit and the actual-delivery requirement

For retail commodity transactions with U.S. persons, CEA §2(c)(2)(D) restricts certain leveraged or financed transactions unless "actual delivery" of the commodity occurs within 28 days. The protocol's design responds to this requirement through the permissionless on-chain ragequit mechanism (Sections 5.4 and 7.5).

A holder of vTokens may, at any time, in a single on-chain transaction, with no operator role and no delay, burn their tokens in exchange for direct ERC-1155 ownership of the pro-rata basket of underlying CTF outcome tokens. The holder's vToken is, by the holder's election, a claim to the underlying tokens themselves. This is actual delivery — in the literal sense that the holder receives the underlying asset into their own wallet — implemented in a way that is far cleaner and more verifiable than any off-chain delivery mechanism applicable to physical commodities.

Ragequit operates regardless of the protocol's daily mint and redeem caps, regardless of any pause state, regardless of operator availability, and regardless of any compliance restriction applied at the frontend. It is the central structural fact of the protocol's compliance posture under U.S. law: the wrapper is not a synthetic claim that the operator promises to settle, but rather a unit-of-account abstraction over directly-owned underlying, convertible to that underlying at the holder's election within a single block.

12.5 Counter-arguments and protocol responses

The commodity-wrapper characterization is the position the protocol takes in good faith on the available authorities. It is not the only available characterization. The principal counter-arguments and the protocol's responses:

Howey investment-contract recharacterization. A regulator could argue that the wrapper itself is an investment contract under *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946),[26] notwithstanding the commodity character of the underlying. The strongest facts for this argument are the pooled basket, the operator's discretion over band selection and weight setting, the operator's execution of basket trades, and the holders' arguable expectation of profits from the operator's efforts. The protocol's responses are: (i) no governance token or other instrument resembling protocol equity exists, removing the most common Howey hook for crypto offerings; (ii) the underlying instruments are themselves commodity interests, putting the wrapper directly on the PAXG/XAUT line of precedent rather than the synthetic-equity recharacterization line; (iii) ragequit converts the wrapper into directly-owned underlying at the holder's election, materially weakening the "efforts of others" and "common enterprise" prongs by eliminating the operator's role at the moment of exit; and (iv) the protocol commits to migrating toward permissionless rebalancing and minting in subsequent versions (Section 13.4), progressively removing operator discretion as an analytical factor.

Security-based swap recharacterization. A regulator could argue that the wrapper falls within the security-based swap definition at Securities Exchange Act §3(a)(68)[27] because its payoff references the eventual

[26] *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946).

[27] Securities Exchange Act of 1934, §3(a)(68) (security-based swap definition).

market valuation of a single identified issuer's equity. The protocol's response is that the wrapper's payoff is a function of CFTC-jurisdictional event-contract prices — binary outcome contracts that the CFTC has consistently treated as swaps under CEA §1a(47) — not of any continuous-value security price directly. The vToken's holder is exposed to the price of those event contracts, traded on a CFTC-licensed DCM, not to Anthropic's equity itself. The economic effect is correlated but the legal character is distinct, and the CFTC/SEC jurisdictional line has historically been drawn at the character of the referenced instrument, not at the economic outcome.

Retail commodity rule (CEA §2(c)(2)(D)). A regulator could argue that the rule's "actual delivery" requirement is not satisfied by ragequit because the holder receives ERC-1155 outcome tokens rather than a physical commodity. The protocol's response is that the rule's policy intent is to prevent off-exchange synthetic exposure to commodities without delivery; the protocol provides on-chain, permissionless, immediate delivery of the underlying digital commodity itself. The 2020 CFTC guidance on retail commodity transactions involving digital assets explicitly contemplates digital-asset delivery as satisfying the rule's policy concern.

The Polymarket-international venue point. A regulator could argue that, to the extent the protocol's vault holds positions acquired from Polymarket's international platform rather than the U.S. DCM, the commodity-wrapper analysis weakens. The protocol's response is that the underlying instrument's character — not the venue's registration — controls the analysis; the CFTC's own 2022 settlement with Blockratize is the agency's contemporaneous characterization of those same instruments as commodity interests; and Polymarket's ongoing migration to U.S.-listed contracts under the QCEX license progressively eliminates this point.

None of these counter-arguments is frivolous. The protocol's posture is that the better reading of the law, taken together with the structural defenses just described, supports the commodity-wrapper characterization. Holders are advised that the position has not been blessed by any regulator and that the analysis is subject to reconsideration as authority develops.

12.6 Other jurisdictions

The legal characterization of vTokens under any non-U.S. legal regime is a question of that regime's local law. The protocol applies KYC and sanctions screening at the frontend and excludes participants from comprehensively sanctioned jurisdictions. Holders in any jurisdiction are responsible for assessing the position under their own jurisdiction's securities, commodities, derivatives, gaming, consumer protection, anti-money-laundering, and tax laws before transacting. The protocol's design is intended to be compatible with the dominant characterization patterns in major financial centers — the European Union's MiCA regime, the United Kingdom's FSMA framework, Singapore's PSA, Hong Kong's SFC regime — but no representation is made about the position in any specific jurisdiction.

---

13 Governance and Operations

13.1 Operating entity

Vaulto Protocol is operated by Vaulto Labs. The operating entity is responsible for backend service availability, signer key management, on-chain administration through the admin multisig, and engagement with regulators, auditors, counterparties, and users. The operating entity is not a counterparty to any vToken; user holdings are claims against the on-chain protocol, not against Vaulto Labs.

13.2 Administrative authority

On-chain administrative authority is held by a Gnosis Safe multisig with `DEFAULT_ADMIN_ROLE` and `ADMIN_ROLE` on each protocol contract. All admin actions other than pause are routed through `VaultoAdminTimelock`, which imposes a 48-hour delay between proposal and execution. The pauser role is held by a separate fast-path EOA (transitioning to a 2-of-3 multisig in production) with no timelock, enabling immediate response to active threats.

The protocol's three operational signing keys (executor, minter signer, oracle pusher) are managed by Vaulto Labs as service operators. Rotation of the minter signer is itself subject to a 24-hour timelock at the contract level, ensuring that even a compromised admin multisig cannot instantly substitute a malicious signer.

13.3 No governance token

There is no Vaulto governance token at the time of this publication and none is planned in the pilot. vTokens are the protocol's product; they are not, and are not intended to be, claims on protocol equity, fee streams, or future governance rights. Any future development of governance mechanisms — whether through a token, a foundation, or some other structure — will be the subject of a separate proposal, separately evaluated for legal and product fit, and not undertaken without explicit communication to the user community.

13.4 Path to decentralization

The pilot is explicitly operator-driven. The protocol does not claim to be decentralized at this stage and does not represent itself as such. Pathways toward greater decentralization in future versions include:

- Permissionless rebalancing — replacing the operator's discretion over band weights with an algorithmic, on-chain process driven by deviation thresholds.
- Permissionless mint — eliminating the off-chain backend signer and allowing any user to construct and submit a valid mint by signing their own receipts against a public NAV.
- Operator-role distribution — moving signing operations from a single Vaulto Labs-controlled service to a threshold network of independent signers.
- Public LP for the secondary market AMM.

These are stated as design directions, not commitments. The pilot's small operating envelope is intentional: it allows the protocol to operate transparently and accumulate evidence about safety properties before broader decentralization.

13.5 Audit and review

Prior to expanding caps beyond pilot levels, the protocol will engage an external smart-contract audit. Audit scope will cover the seven contracts in the tokenization stack and the integration surface against Polymarket V2. The audit report will be published.

Subsequent code changes — fee adjustments, new company onboarding, AMM v2 deployment — will follow standard change-management discipline including review, testing, and (where material) re-audit before promotion to production.

---

14 Roadmap

The protocol's development is organized around four phases. Dates are intentionally omitted; the protocol will advance through phases as engineering and regulatory work allows, not on a fixed calendar.

Phase 0 — Contracts (complete). Smart contracts written, locally tested (42 of 42 Foundry tests passing), and verified against forked Polygon state.

Phase 1 — Backend integration (current). Off-chain orchestration for mint, redeem, oracle pushing, and reconciliation. EIP-1271 / `POLY_1271` signing path for Polymarket V2 integration. Internal vitest coverage.

Phase 2 — Pilot launch. Mainnet deployment with $100/day cap, internal team testing, then opt-in cohort of external users under the Reg S framework. Operating period intended to be at least four weeks before any cap increase. Solvency invariant monitored continuously.

Phase 3 — Audit and expansion. External smart-contract audit. Post-audit, raise daily caps and broaden the operating cohort. Begin onboarding additional companies — the remaining 16 Polymarket events already supported by Vaulto's existing trading infrastructure are the natural pipeline. Deploy the Uniswap V3 secondary market.

Phase 4 — Decentralization and broader product surface. Public LP for the AMM. Permissionless rebalancing. Permissionless mint. Multi-chain deployment. Integration with downstream DeFi (lending markets, structured products, index protocols).

Throughout all phases, the protocol maintains the always-on ragequit path and the publication of the solvency invariant. No development direction is permitted to compromise those two structural commitments.

---

15 Glossary and References

15.1 Glossary

Band. One of the disjoint outcome ranges of a Polymarket multi-outcome event. For the Anthropic IPO event, bands correspond to ranges of the company's eventual IPO closing market capitalization.

Basket. The collection of CTF YES outcome tokens, with associated weights, that backs a vToken.

CTF. Conditional Token Framework. Gnosis's smart contract standard for outcome tokens, used by Polymarket as the on-chain representation of binary outcome positions. Implemented as an ERC-1155 token at `0x4D97DCd97eC945f40cF65F87097ACe5EA0476045` on Polygon.

DCM. Designated Contract Market. A CFTC-licensed venue for trading commodity derivatives, including event contracts. Polymarket US operates under a DCM license inherited through the July 2025 acquisition of QCEX.

EIP-1271. The Ethereum standard for smart-contract signature validation, allowing a contract to declare a signature valid via the `isValidSignature(bytes32, bytes)` interface.

EIP-712. The Ethereum standard for typed-data signatures, used by Vaulto's mint and redeem receipts and by Polymarket's V2 order signing.

Mint receipt. An EIP-712-signed message issued by the protocol's minter signer attesting to the parameters of a single mint operation. Verified on-chain by `MintRedeemController`.

NAV. Net asset value per vToken, computed as the weighted average of basket band TWAP prices in USDC.

negRisk. Polymarket V2's negative-risk multi-outcome event structure, in which YES outcome tokens across all bands sum to no more than one dollar.

POLY_1271. Polymarket V2 signature type 3, indicating that the order maker is a smart contract that implements EIP-1271. Used by `CompanyVault` for Polymarket V2 order authorization.

pUSD. Polymarket V2's settlement collateral asset on Polygon, at `0xC011a7E12a19f7B1f670d46F03B03f3342E82DFB`. Pegged 1:1 to USDC.e through the Polymarket Collateral Onramp.

Ragequit. The protocol's permissionless on-chain exit mechanism. A vToken holder burns their tokens to receive the pro-rata share of the underlying basket directly, with no operator involvement and no fee.

Commodity interest. An instrument falling within CFTC jurisdiction under the Commodity Exchange Act, including commodity futures, options, and swaps. Polymarket CTF outcome tokens are commodity interests under CEA §1a(47).

Commodity-derivative wrapper. A token that wraps an underlying commodity interest in a redeemable representation and inherits the underlying's commodity character. Examples: PAXG (gold), XAUT (gold), Vaulto vTokens (Polymarket event contracts).

DCO. Derivatives Clearing Organization. A CFTC-registered entity that clears trades on a DCM. Polymarket US operates a DCO license inherited through the QCEX acquisition.

TWAP. Time-weighted average price. Vaulto computes a 5-observation, 60-second cadence TWAP from pushed Polymarket CTF mid-prices.

`vCOMPANY_L` / `vCOMPANY_S`. Vaulto's long and short vTokens for a given referenced company. Pilot: `vANTHROPIC_L` and `vANTHROPIC_S`.

Valuation band. A range of possible eventual IPO closing market capitalizations for a referenced company. For Anthropic, bands span from less than $100B to $900B+, plus a "no IPO by resolution date" band.

15.2 References

Smart contracts and standards.

- ERC-20. *EIP-20: Token Standard.* Fabian Vogelsteller, Vitalik Buterin, 2015. https://eips.ethereum.org/EIPS/eip-20
- ERC-1155. *EIP-1155: Multi Token Standard.* Witek Radomski et al., 2018. https://eips.ethereum.org/EIPS/eip-1155
- ERC-1271. *EIP-1271: Standard Signature Validation Method for Contracts.* Francisco Giordano, Matt Condon, 2018. https://eips.ethereum.org/EIPS/eip-1271
- ERC-2612. *EIP-2612: Permit – 712-signed Approvals.* Martin Lundfall et al., 2020. https://eips.ethereum.org/EIPS/eip-2612
- Gnosis Conditional Token Framework. https://docs.gnosis.io/conditionaltokens/
- OpenZeppelin Contracts v5.1. https://docs.openzeppelin.com/contracts/5.x/
- Uniswap V3 Core. https://uniswap.org/whitepaper-v3.pdf

Polymarket and the CFTC.

- Polymarket Acquires QCEX. *PR Newswire,* July 2025. https://www.prnewswire.com/news-releases/polymarket-acquires-cftc-licensed-exchange-and-clearinghouse-qcex-for-112-million-302509626.html
- Polymarket Receives CFTC Approval of Amended Order of Designation. *PR Newswire,* November 2025. https://www.prnewswire.com/news-releases/polymarket-receives-cftc-approval-of-amended-order-of-designation-enabling-intermediated-us-market-access-302625833.html
- CFTC Order on Blockratize (Polymarket). PR 8478-22, 2022. https://www.cftc.gov/PressRoom/PressReleases/8478-22

- *KalshiEX LLC v. CFTC,* No. 24-5205 (D.C. Cir. 2024). https://media.cadc.uscourts.gov/opinions/docs/2024/10/24-5205-2077790.pdf
- Event Contracts NPRM, 89 Fed. Reg. 48968 (June 2024). https://www.federalregister.gov/documents/2024/06/10/2024-12125/event-contracts
- Commodity Exchange Act, 7 U.S.C. §§1 et seq.
- Polymarket Conditional Tokens documentation. https://docs.polymarket.com/

SEC guidance and case law.

- *SEC v. W.J. Howey Co.,* 328 U.S. 293 (1946).
- *SEC v. Reves,* 494 U.S. 56 (1990).
- *SEC v. Terraform Labs,* No. 23-cv-1346 (S.D.N.Y. 2024).
- SEC Chair Paul S. Atkins, "Project Crypto" (November 2025). https://www.sec.gov/newsroom/speeches-statements/atkins-111225-secs-approach-digital-assets-inside-project-crypto
- Securities Act of 1933, Regulation S. 17 C.F.R. §§ 230.901–230.905.
- Securities Exchange Act of 1934, §3(a)(68) (security-based swap definition).

Comparable tokenized-instrument whitepapers.

- Ondo Finance USDY documentation. https://docs.ondo.finance/general-access-products/usdy/basics
- Pendle Finance protocol documentation. https://docs.pendle.finance/
- Backed Finance product documentation. https://backed.fi/
- Maple Finance documentation. https://maplefinance.gitbook.io/maple
- Frax Finance v1 protocol documentation. https://docs.frax.finance/

End of Whitepaper. Version 0.1. May 2026.