



Avora Finance

Self-custody trading, verified social activity and
copy trading on Robinhood Chain

NETWORK

Robinhood Chain · 4663

CUSTODY

User-held keys

SETTLEMENT

Verified on-chain

STATUS

Live

Technical Whitepaper

Version 0.1 · September 2026

This document describes software as built and as planned at the date above. It is not an offer of securities, investment advice or a solicitation. Features marked "Next" or "Later" are not available and may change or not ship. Avora has not issued a token.

Contents

Abstract	2
1 Motivation	2
2 Design principles	2
3 System overview	3
4 Identity and sessions	3
5 Trading	4
5.1 Quoting and routing	4
5.2 Preflight checks	4
5.3 Intent lifecycle	4
5.4 Receipt verification	4
5.5 Protected swaps	5
5.6 Private swaps	5
6 Verified social layer	5
7 Copy trading	6
7.1 Manual copy (v1) LIVE	6
7.2 Automatic copy NEXT	6
8 Earn: USDG yield	6
9 Stock Tokens	7
10 Security model	7
11 Fees	8
12 Roadmap	8
13 Risks	9
14 References	9
Appendix: contract addresses	9

Abstract

Avora Finance is a self-custody web application on Robinhood Chain for trading crypto assets and tokenized equities (“Stock Tokens”), following other traders, copying their trades within user-defined limits, and earning yield on the USDG stablecoin. Users keep their own keys: every transaction is signed in the user’s wallet, and the platform cannot move funds.

The central design choice is that **nothing counts until it is verified on-chain**. A trade enters a user’s portfolio, public feed, leaderboard standing or a follower’s copy alert only after an independent worker has confirmed the transaction receipt against the exact calldata the platform built. Performance on Avora cannot be self-reported, and the social layer cannot be seeded with fabricated results.

This paper describes the system as it runs today: identity and sessions, the swap and settlement pipeline, the verified social and copy layer, USDG yield through established vaults, and the security model. It then separates clearly what is live from what is planned, and lists the risks a user takes on.

SECTION 1

Motivation

On-chain trading is spread across many tools. A trader uses one app to swap, a block explorer to check what happened, a group chat or social feed to find ideas, and a separate protocol to put idle stablecoins to work. Tokenized equities on Robinhood Chain add a new asset class to that picture, with market hours, halts and issuer controls that generic swap interfaces do not handle.

Social and copy trading in crypto has a further problem: **trust in reported results**. Leaderboards built on screenshots, self-reported PnL or custodial account balances are easy to game. Copy-trading products that work by pooling user funds ask users to give up custody for access to a strategy.

Avora addresses both problems with one application in which:

- every trade is a transaction or order the user signs from their own wallet;
- trader performance is derived only from settled, verified on-chain trades;
- copying a trader produces a pre-filled trade that stays within limits the copier set, and the copier still signs it.

SECTION 2

Design principles

Self-custody first

Users sign every transaction. The platform holds no user keys and has no contract that can take custody of user funds.

Proof over claims

Positions, posts, leaderboards and copy alerts are built only from receipts verified on-chain. We do not publish numbers we cannot prove.

The user controls the risk

Slippage limits, balance and gas checks, market-hours checks and copy caps run before a user is ever asked to sign.

One place

Trading, discovery, copying and yield are parts of one flow in one app, not a bundle of separate products.

SECTION 3

System overview

Avora is made of a web client, an API, a background worker and a database, reading from and verifying against Robinhood Chain. The client talks to the user's wallet; the API never signs on the user's behalf.

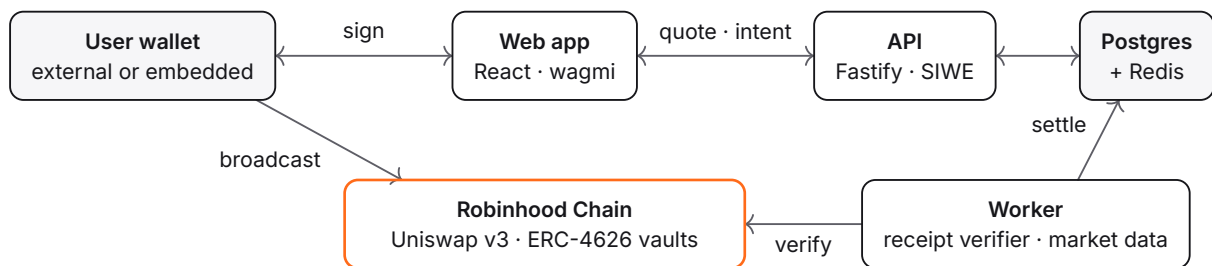


Figure 1: The user's wallet is the only component that signs. The worker verifies against the chain before writing results.

Component	Role
Web app	React 19 and wagmi/viem. Connects an external wallet (MetaMask, Rabby, WalletConnect, Coinbase Wallet) or a self-custodial embedded wallet created at email sign-in (Privy).
API	Sign-In with Ethereum sessions, markets, quotes, preflight checks, trade intents, social graph, copy policies, notifications.
Worker	Receipt verification and settlement, asset registry sync, crypto and Stock Token market data, feed fan-out, copy alerts, leaderboard.
Chain	Robinhood Chain (chain ID 4663), an Arbitrum Orbit L2 with blocks about every 100 ms and gas paid in ETH.

SECTION 4

Identity and sessions

A user signs in by proving control of a wallet with **Sign-In with Ethereum** (EIP-4361). The same flow works for external wallets and embedded wallets, so the backend does not depend on any one wallet provider.

- The signed message is bound to the Avora domain, URI and chain ID. Mismatches are rejected.
- Each nonce is single-use and expires after five minutes. Under concurrent replay of one nonce, exactly one verification succeeds (tested with 20 parallel attempts).
- The session is an httpOnly, Secure, SameSite=Lax cookie. The sign-in message states that it costs no gas and moves no funds.

- A user can link several wallets, each proven by its own signature.

SECTION 5

Trading

Avora routes swaps through Uniswap v3 on Robinhood Chain. The platform builds and checks the transaction; the user's wallet signs and broadcasts it; the worker verifies the result.

5.1 Quoting and routing

Quotes come from Uniswap's QuoterV2 across all four fee tiers (0.01%, 0.05%, 0.3%, 1%), with two-hop routes through WETH or USDG when there is no deep direct pool. Assets are tradeable only when a pool with real liquidity exists. Quotes expire after 30 seconds.

5.2 Preflight checks

Before a user is asked to sign, the API runs checks in a fixed order and stops at the first failure with a readable reason:

#	Check
1	The wallet belongs to the signed-in session
2	Both assets are registered and tradeable
3	Amount and decimals are valid
4	The on-chain balance covers the amount
5	An ETH reserve remains for gas
6	Stock Tokens: the market is open, and the token is not halted, <code>paused()</code> or oracle-paused
7	A route exists and its output simulates successfully from the user's address
8	Price impact is within limits (above 5% is blocked); slippage and fees are shown, with a minimum received

5.3 Intent lifecycle

Each trade is an **intent** with a strict state machine. State changes use conditional updates (`UPDATE ... WHERE status = ...`), so concurrent requests cannot move one intent twice.

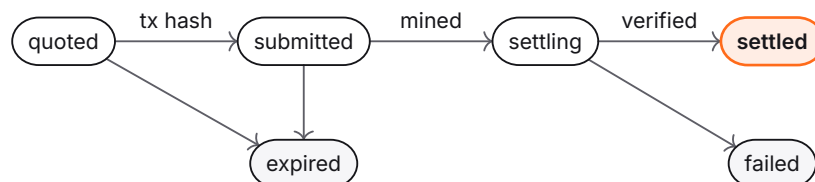


Figure 2: An intent reaches `settled` only after the receipt verifier accepts it.

At submission the API re-quotes and re-simulates; if output has fallen below the user's minimum, it returns `PRICE_MOVED` instead of letting the user sign a transaction that would revert. Router deadlines are at most 120 seconds. Submission is idempotent: a retried request replays the stored response rather than creating a second trade.

5.4 Receipt verification

The client reports a transaction hash, but the platform does not trust that report. The worker accepts a transaction only if all of the following hold:

1. the sender is the wallet the intent was created for;
2. the recipient is the Uniswap SwapRouter02 contract;
3. the calldata matches the intent byte for byte (route, input amount, minimum output);
4. the receipt status is success;
5. the transaction has the configured number of confirmations (default 20) and its block hash still matches, which guards against reorgs.

Actual amounts are read from the token Transfer logs, not from the quote. A transaction hash can bind to only one intent. Forged, mismatched and reorged transactions are covered by tests run against a fork of Robinhood Chain.

5.5 Protected swaps

Robinhood Chain's sequencer orders transactions first-come, first-served, with no public mempool and no priority gas auctions, so sandwich attacks are largely designed out at the chain level. Avora adds tight slippage limits, short deadlines and pre-sign simulation. We call these swaps **protected**, not **private**: amounts and addresses are public on-chain.

5.6 Private swaps

For token-to-token trades, Avora also requests a price from UniswapX solvers. If a solver matches or beats the protected-swap price, the trade goes **private**: the user signs an off-chain order (via Permit2, approving exactly the amount sold) instead of broadcasting a transaction. A solver fills the order, pays the network fee and delivers the tokens to the user's wallet. The UniswapX reactor contract enforces the minimum received, so the order fills within the user's terms or not at all.

The order stays off the public transaction flow until it settles. Settlement is verified the same way as a swap: the worker must find the reactor's Fill event for that exact order hash and wallet, with the required confirmations and a reorg recheck, before the trade counts. Unfilled orders expire after a few minutes and nothing is exchanged. Small trades and trades that start or end in ETH use a protected swap, and the swap screen shows which path applies before signing.

SECTION 6

Verified social layer

Traders can publish a profile, post a thesis, and share trades. What makes the feed useful is what it refuses to show:

- **Trade posts exist only for settled trades.** A post cannot claim a trade the verifier has not confirmed.
- **Publication can be delayed** by the trader, so followers see a trade after the fact rather than front-running it.
- **Leaderboards count confirmed trades only.** There is no way to submit a result by hand.
- **Privacy is the trader's choice.** Profiles can require follow approval; users can block and report.

Because every entry is linked to a transaction, anyone can check a leaderboard position against the chain.

SECTION 7

Copy trading

7.1 Manual copy (v1) LIVE

A user creates a **copy policy** for a trader with their own limits: amount per trade, daily cap, maximum open copies and maximum slippage. When the trader settles a trade, followers with a policy receive an alert and a one-tap, pre-filled trade sized within their limits. The follower reviews it and signs it from their own wallet.

Limits are enforced on the server under a row lock, so concurrent alerts cannot exceed a cap (tested with 50 concurrent prefills). Each source trade can produce at most one copy per policy.

7.2 Automatic copy NEXT

Automatic copying without a signature per trade requires delegated, scoped permissions rather than custody. Robinhood Chain supports EIP-7702 and ERC-4337. The planned design delegates an embedded wallet to an audited smart-account module with **session keys** capped by amount, asset list, slippage and expiry, revocable by the user at any time. Avora would still hold no keys that can move funds outside those caps.

SECTION 8

Earn: USDG yield

Avora lets users deposit USDG into established ERC-4626 vaults already deployed on Robinhood Chain. The deposit goes from the user's wallet straight into the vault; the user holds the vault shares and can withdraw at any time, subject to the vault's own liquidity. Avora deploys no contract in this path and takes no fee.

Vault	Protocol / curator	Risk profile
Spark Savings USDG	Spark	Savings rate set by Spark governance; deposit cap; smart-contract and stablecoin risk.
Steakhouse USDG	Morpho · Steakhouse Financial	Lends USDG in curator-selected Morpho markets; variable rate; lending, liquidation and smart-contract risk.
Ethena × Steakhouse USDG	Morpho · Steakhouse Financial	Lends USDG against Ethena collateral; variable rate; lending, liquidation and smart-contract risk.

The app shows each vault's live base APY read from its source. Some vaults advertise boosted rates that apply only to whitelisted users; Avora does not show those as the rate a user will receive.

SECTION 9

Stock Tokens

Stock Tokens are tokenized equities issued on Robinhood Chain. Avora syncs the issuer's public registry (about 195 tokens at the time of writing) and its bid/ask prices, and it handles their controls explicitly:

- **Market hours and halts:** trades are blocked when the market is closed or the symbol is halted.
- **Issuer controls:** tokens are upgradeable proxies that can be paused or blocklisted. Preflight reads `paused()` and oracle status before quoting, so the user gets a clear message instead of a failed transaction.
- **Access policy:** access is currently open. The platform includes a compliance hook (per-asset restriction and an attestation step) so access can be restricted by jurisdiction if required. Users are responsible for whether holding these tokens is permitted where they live.

SECTION 10

Security model

Avora can	Avora cannot
Build a transaction and show it to the user	Sign or broadcast a transaction for a user
Refuse to quote or record a trade	Move, freeze or withdraw user funds
Hide a post or profile from its own feed	Change what happened on-chain
See wallet addresses linked to an account	Access private keys (external or embedded)

Other controls:

- Operator actions are restricted to a fixed set of addresses and written to an audit log.
- Rate limits apply per user and per IP; logs are redacted.
- Money is stored as integer base units (`Decimal(78,0)`) and crosses the API as strings, so there is no floating-point rounding.
- Only the canonical USDG contract is accepted; a lookalike token on the chain is excluded by address.
- The test suite runs against a local fork of Robinhood Chain, with real signed swaps and deposits.

Trust assumptions

Users trust their wallet provider, Robinhood Chain's sequencer and bridge, Uniswap v3, the vault protocols they choose, and the issuers of the tokens they hold. They trust Avora to display accurate quotes and history, but every transaction is shown in their wallet before signing and can be checked on the [block explorer](#).

SECTION 11

Fees

At launch Avora charges **no platform fee** on swaps, copies or Earn deposits. Users pay:

- the Uniswap v3 pool fee of the route (0.01% to 1%, shown before signing);
- network gas in ETH (on private swaps the solver pays it, and the price already includes it);
- any fees charged by a vault they deposit into.

If a platform fee is introduced, it will be shown in the quote before signing and announced in a revised version of this paper.

SECTION 12

Roadmap

The roadmap is split by what each item requires. Items that need Avora's own smart contracts will not ship before an independent audit.

Status	Item	Needs own contracts
LIVE	Self-custody accounts, SIWE sessions, linked wallets	No
LIVE	Protected swaps: crypto and Stock Tokens via Uniswap v3	No
LIVE	Private swaps filled by UniswapX solvers, gasless for the user	No
LIVE	Verified feed, profiles, leaderboards	No
LIVE	Manual copy trading with limits	No
LIVE	Earn: USDG in Morpho and Spark vaults	No
NEXT	Liquidity provision UI for Uniswap v3 pools	No
NEXT	Automatic copy trading with scoped session keys	No (audited modules)
LATER	Rewards programme	Possibly · audit first
LATER	Governance	Yes · audit first
LATER	Bonded solver network	Yes · audit first

On a token

Avora has not issued a token and has not announced one. Any token-related feature would be described in a revised version of this paper, with its contracts published and audited before launch. Treat any token presented as Avora's without that as unofficial.

SECTION 13

Risks

- **Smart-contract risk.** Uniswap v3, the vaults and the tokens themselves are third-party contracts. Bugs or exploits in them can cause loss.
- **Stablecoin and issuer risk.** USDG and Stock Tokens can be paused, frozen or blocklisted by their issuers. A Stock Token tracks, but is not, the underlying share.
- **Market risk.** Prices move. Copying a trader copies their losses as well as their gains; past on-chain results do not predict future ones.
- **Yield risk.** Vault rates are variable and can fall to zero; lending vaults can take losses from bad debt.
- **Chain risk.** Robinhood Chain is a young L2 with a centralized sequencer. Downtime, reorgs or bridge issues affect every app on it.
- **Wallet risk.** A lost or compromised key cannot be recovered by Avora.
- **Regulatory risk.** Rules for tokenized equities and on-chain trading differ by jurisdiction and are changing.

SECTION 14

References

- Robinhood Chain documentation: contracts, account abstraction, oracles. <https://docs.robinhood.com/chain>
- Uniswap v3 deployments on chain 4663: [Uniswap/contracts, deployments/json/4663.json](https://github.com/Uniswap/contracts-deployments/blob/main/json/4663.json).
- EIP-4361, Sign-In with Ethereum. <https://eips.ethereum.org/EIPS/eip-4361>
- ERC-4626, Tokenized Vaults. <https://eips.ethereum.org/EIPS/eip-4626>
- EIP-7702 and ERC-4337, account abstraction.
- Morpho on Robinhood Chain. <https://app.morpho.org/robinhood-chain>
- Spark. <https://app.spark.fi>

Appendix: contract addresses

All addresses are on Robinhood Chain (chain ID 4663) and were checked for deployed bytecode.

Contract	Address
WETH	0x0Bd7D308f8E1639FAB988df18A8011f41EAcAD73
USDG (Global Dollar, 6 decimals)	0x5fc5360D0400a0Fd4f2af552ADD042D716F1d168
Uniswap v3 Factory	0x1f7d7550b1b028f7571e69a784071f0205fd2efa
Uniswap QuoterV2	0x33e885ed0ec9bf04ecfb19341582aadcb4c8a9e7
Uniswap SwapRouter02	0xcaf681a66d020601342297493863e78c959e5cb2
Permit2	0x000000000022D473030F116dDEE9F6B43aC78BA3
Multicall3	0xcA11bde05977b3631167028862bE2a173976CA11
Chainlink ETH/USD	0x78F3556b67E17Df817D51Ef5a990cDaF09E8d3A9
Chainlink USDG/USD	0x61B7e5650328764B076A108EFF5fa7282a1B9aD2
Spark Savings USDG	0xde770c84FE66E063336b31737cFE9790f18c4087
Steakhouse USDG (Morpho)	0xBeeFF033F34C046626B8D0A041844C5d1A5409dd
Ethena x Steakhouse USDG (Morpho)	0xbEeFF0fb1Dc19344A87b8479dAb60A2e16160737