VEIL

The private financial layer for Robinhood Chain

Whitepaper v1.0

Version 1.0

Status: Testnet-stage. Mainnet targeted for Q3 2026.

TL;DR

Veil is the private financial layer for Robinhood Chain. It lets anyone move, receive, swap, and spend value without broadcasting amounts or the link between sender and receiver to the entire network. Funds stay in your control at all times because Veil is non-custodial and your keys never leave your wallet. When you deposit into Veil, your public balance becomes an encrypted private note, and every action after that is proven with zero-knowledge cryptography, so the chain confirms that a transaction is valid without ever seeing what it contains. The same architecture is open to other Robinhood Chain tokens, which means any supported project can offer its holders real privacy without building any of it themselves.

Who Veil is for

Veil is built for people and businesses that need normal financial privacy on a public blockchain. That includes individuals who simply do not want their salary, savings, and spending exposed to anyone who looks up their address. It includes merchants who want to accept crypto without publishing their revenue to competitors. It includes payroll teams that need to pay contributors without turning every wallet into a public compensation report. It includes traders and treasuries that want to rebalance without telegraphing their moves, and it includes builders who want their token to feel private out of the box. If you would not post your bank statement in public, Veil is for you.

Executive Summary

Public blockchains made a deliberate trade. To let anyone verify the ledger, they made the ledger visible to everyone. That transparency is what secures the network, but it also means that every transfer, balance, and counterparty is permanently readable by anyone with a block explorer. For a settlement layer that aims to carry real payments, commerce, and finance, this is a serious problem. Financial privacy is not a niche demand. It is the default expectation everywhere money already moves.

Veil closes that gap on Robinhood Chain. It is a privacy protocol that sits on top of the chain and gives users a shielded space where value can move confidentially. The mechanism is straightforward in spirit. You deposit public funds into a non-custodial shielded pool, and in return the protocol records an encrypted private note that only you can spend. From that point forward, your actions are expressed as zero-knowledge proofs. A proof convinces the network that you own a valid note and that you are not double-spending, while revealing nothing about the amount, the origin, or the destination. Nullifiers ensure each note can be spent exactly once, and the pool contract enforces all of this on-chain.

Because Veil is non-custodial, your keys stay in your wallet and the protocol never takes control of your funds. There are no protocol-imposed withdrawal delays. Value can enter and leave the shielded pool on your schedule. Robinhood Chain gives Veil a fast, low-fee, EVM-compatible base to build on, and Veil gives Robinhood Chain the missing layer that turns a transparent ledger into a usable private financial system.

The Privacy Gap on Robinhood Chain

Robinhood Chain is fast, inexpensive, and EVM-compatible, which makes it an excellent foundation for payments and consumer finance. But it inherits the same structural exposure as every other public chain. When you send funds, the amount is visible. When you receive funds, the source is visible. Your entire history is linked to a single address that anyone can inspect forever.

In practice this creates real harm. A person who is paid on-chain reveals their income to their landlord, their employer's competitors, and anyone who happens to have their address. A shop that accepts on-chain payments publishes its daily takings. A team that pays contributors exposes each person's rate to everyone else on the team. Even ordinary users become targets once a wallet with a meaningful balance is tied to a real identity. Transparency was meant to protect the network. It ends up leaving the people who use it fully undressed.

The gap is not that privacy tools are impossible. It is that, until now, there has been no native, non-custodial, easy-to-use privacy layer designed specifically for Robinhood Chain and its tokens. Veil exists to be exactly that.

Design Principles

1. **Privacy by cryptography, not by trust.** Confidentiality is enforced with zero-knowledge proofs and on-chain verification. It does not depend on a company keeping a promise or a server behaving well.

2. **Non-custodial by default.** Your keys never leave your wallet. Funds sit in a shielded pool that no operator can seize, freeze, or spend on your behalf.

3. **No artificial delays.** Veil imposes no protocol-level lockups or withdrawal timers. Value moves in and out of the shielded pool when you decide.

4. **Familiar to use.** Privacy should feel like a normal wallet action. Deposit, send, receive, swap, and withdraw are presented as simple steps, with the cryptography handled behind the scenes.

5. **Verifiable without exposure.** The network can always confirm that a transaction is valid. It just cannot see the private details. Validity and privacy are not in conflict.

6. **Open to the ecosystem.** The same shielded architecture is reusable by other Robinhood Chain tokens, so privacy becomes a shared public good rather than something each project rebuilds alone.

Protocol Architecture

Veil is organized into a frontend layer that runs in the user's browser and a blockchain layer that lives on Robinhood Chain. Together they let a user act privately while the chain stays the final source of truth.

Frontend layer

The frontend is the Veil dApp. It connects to the user's wallet, holds encrypted note data locally, and assembles the information a proof needs.

- **Wallet Connect.** The dApp connects through MetaMask and helps the user switch to Robinhood Chain. Connection is used for signing and for reading balances, never for handing custody to the protocol.

- **Encrypted Note Storage.** Private notes are stored encrypted in the browser. They are unlocked by a wallet signature, so only the person holding the wallet can read or spend them.
- **Indexer.** The indexer tracks the data the dApp needs to stay in sync, including commitments, Merkle roots, spent nullifiers, supported assets, and overall sync status. The Home screen surfaces indexer health so users know their view is current.
- **Merkle Witness Lookup.** To prove a note exists without exposing its secret, the dApp fetches the Merkle proof path for that note. This witness is fed into the proof, letting the user demonstrate membership in the pool while keeping the note itself private.
- **Proof Service.** The proof service generates the zero-knowledge proofs behind each private action, including private sends, public exits (withdrawals), and private swaps. It turns the user's intent and secret data into a proof the contract can verify.

Blockchain layer

The blockchain layer is where privacy is enforced and settled.

- **VeilPool Contract.** This is the heart of the system. It stores commitments, verifies incoming proofs, tracks nullifiers, and prevents double-spending. Nothing enters or leaves the shielded pool without satisfying the contract's checks.
- **Nullifier Protection.** Every note carries a unique nullifier that is published when the note is spent. Because the contract rejects any nullifier it has already seen, a note can be spent once and only once, even though the amount and parties stay hidden.
- **Asset Registry.** The registry defines which tokens are allowed inside the private pool. It is the gate that lets Veil support multiple assets in a controlled way.

Extensibility and multi-asset support

Veil was designed as shared infrastructure, not a single-token product. The Asset Registry lets the protocol admit additional Robinhood Chain tokens into the same shielded pool architecture. A new token does not require a new privacy system. It reuses the same commitments, the same nullifier logic, and the same zero-knowledge verification, while inheriting the same non-custodial guarantees. This is what makes token integrations practical. Privacy becomes a capability that any supported asset can switch on, rather than a bespoke project each team has to fund and secure on its own.

Zero-Knowledge Privacy Layer

Zero-knowledge proofs are the reason Veil can be both private and verifiable. A zero-knowledge proof lets one party prove a statement is true without revealing why it is true. In Veil, the statement is roughly this: "I own a valid, unspent note in the pool, and the transaction I am submitting is correctly formed." The proof convinces the VeilPool contract of exactly that, and nothing else.

When you deposit, the protocol records a commitment, which is a cryptographic fingerprint of a private note. The commitment reveals nothing about the amount or the owner. When you later spend that note, you produce a proof that references the note's place in the pool's Merkle tree through the witness path, publish the note's nullifier so it cannot be reused, and create one or more new commitments for the recipients. The contract checks the proof, confirms the nullifier is fresh, and updates its state. At no point does the chain learn the amount, the sender, or the receiver. It only learns that the rules were followed.

The result is a system where privacy is not a policy that can be relaxed and validity is not a claim that has to be trusted. Both are properties of the mathematics. The network can always tell that a transaction is legitimate, and it can never tell what the transaction actually said.

Core Features and Transaction Lifecycle

The dApp menu

The Veil dApp presents its capabilities as clear actions:

- **Home.** Wallet status, balances, private note counts, and indexer health at a glance.
- **Deposit.** Move public funds into the shielded pool, turning them into a private note.
- **Private Send.** Send value privately to another user.
- **Private Receive.** Receive value into a new private note.
- **Private Swap.** Swap one supported asset for another without exposing the trade.
- **Gasless Swap.** A smoother swap flow where gas handling is simplified for the user.
- **Withdraw.** Exit the pool back to a public balance.
- **Private Buy** and **Private Sell.** Enter and exit positions privately.

Transaction lifecycle: a private transfer from A to B

The clearest way to understand Veil is to follow value from one person to another.

1. **A deposits.** Alice deposits public funds into Veil. Her public balance becomes an encrypted private note that only she can spend.

2. **A chooses Private Send.** Alice selects Private Send and enters Bob's receiving details.

3. **Veil generates a proof.** The dApp produces a zero-knowledge proof that Alice owns a valid note, using the Merkle witness to show the note exists in the pool without revealing its secret.

4. **The old note is nullified.** Alice's original note is marked as spent through its nullifier, which the VeilPool contract records so the note can never be spent again.

5. **B receives a new note.** Bob receives a fresh encrypted private note representing the value Alice sent. The chain confirms the transfer was valid without learning the amount or the link between Alice and Bob.

6. **B decides what to do next.** Bob can keep the note, send it onward, swap it, or withdraw it to a public balance whenever he chooses.

Throughout this flow, custody never changes hands to the protocol, no amounts are exposed, and there is no imposed waiting period.

Gasless Execution Model

Even with strong cryptography, privacy fails if it is too awkward to use. One of the sharpest edges for new users is gas. Managing a separate balance for fees, timing transactions, and understanding gas at all can be enough friction to push people back toward transparent tools.

Veil's gasless execution model smooths this out. For swaps and transfers, gas handling is simplified so that private actions feel effortless and close to how people already expect payments to work. The important detail is that this convenience does not reintroduce custodial risk. Simplifying the fee experience does not mean handing over your keys or your funds. Custody stays with the user, the shielded pool stays non-custodial, and the security guarantees of the protocol are unchanged. The goal is a private action that feels as natural as any everyday payment, without quietly trading away the properties that make Veil trustworthy.

Ecosystem and Token Integrations

Veil is more than a single application. It is a privacy layer that other products and tokens can build on.

The ecosystem includes Private Payments for everyday confidential transfers, Veil Check+ for sending value like cash, Merchant Payments for businesses that want to accept crypto without publishing revenue, Payroll for paying teams and contributors privately, AI Agent Payments for autonomous software that transacts on a user's behalf, Stablecoin Rails for private movement of stable value, OTC and Treasury tools for larger and more sensitive flows, and Wallets and SDK support so that developers can embed Veil directly into their own products.

Token Integrations are central to this vision. Supported Robinhood Chain tokens can integrate with Veil so that their holders gain the same privacy features through the dApp, without each project having to build and secure its own privacy infrastructure. A new token that integrates reuses the same shielded pool, the same commitment and nullifier design, and the same zero-knowledge verification that already power Veil. It inherits the same security posture and the same non-custodial custody guarantees. This turns privacy into shared infrastructure for the whole chain. Instead of a landscape where only a few well-funded teams can afford real confidentiality, any supported token can offer it, and every integration strengthens the shared shielded pool that all of them draw on.

Veil Check+

Veil Check+ makes sending value feel like handing someone cash. The flow is simple. The sender chooses **Create Check**, which produces a **QR Code**, a **Claim Code**, and a shareable **Private Link**. The recipient uses any of these to claim the value, and on **Recipient Claims** the funds land in a brand new private note under their control. No wallet addresses are exchanged and no amounts are exposed. It is the closest on-chain equivalent to passing someone a folded banknote.

Security and Audits

Security in Veil is enforced at the level of cryptography and contract logic, not policy. Privacy comes from zero-knowledge proofs, which mean the network verifies validity without seeing private data. Nullifier protection prevents double-spends by guaranteeing each note is spendable exactly once. Notes are stored encrypted and unlocked only by a wallet signature, so local data is not readable by anyone but the owner. All spending rules are enforced on-chain by the VeilPool contract, and custody remains with the user at every step because the protocol is non-custodial.

We want to be direct about the state of external review. Independent third-party audits and hardening are part of the path to the Q3 2026 mainnet. These audits are planned and ongoing, not finished, and we

will not claim otherwise. Alongside audits, the security posture includes a bug bounty, open-source code that anyone can inspect, and a responsible disclosure process so that researchers can report issues safely. Cryptographic systems earn trust through scrutiny over time, and Veil is being built to invite that scrutiny rather than avoid it.

Token Model and Economics

The VEIL token is the utility token that powers the Veil ecosystem. It is issued on Robinhood Chain with a fixed total supply of 1,000,000,000 VEIL.

VEIL has five core utilities:

- **Private swaps.** VEIL is used within the private swap flows that let users trade supported assets confidentially.
- **Private transfers.** VEIL supports the confidential transfer of value between users.
- **Protocol fees.** VEIL is used to pay the fees that keep the protocol running.
- **Ecosystem incentives.** VEIL is used to reward the participants and integrations that grow the shielded pool and the wider ecosystem.
- **Future governance.** VEIL is intended to give holders a voice in the protocol's direction as governance is introduced over time.

The token is designed to align the people who use Veil, the projects that integrate with it, and the long-term health of the protocol. As more tokens integrate and more value flows through the shielded pool, the utility of VEIL grows with the network it secures.

Roadmap

Q3 2026, Ecosystem Expansion and Mainnet Launch. The central milestone is the Robinhood Chain mainnet launch. At mainnet, Veil delivers private transfers, private swaps, gasless swaps, deposits, withdrawals, and transaction history as a complete private financial workflow. In the same phase, Veil enables supported Robinhood Chain tokens to integrate with the protocol and begins onboarding selected ecosystem tokens into the shared shielded pool. Independent audits and hardening continue through this period as part of the path to mainnet.

Q4 2026, Merchants and Developers. The focus shifts to bringing Veil to businesses and builders through merchant tools for accepting private payments and a developer SDK that lets teams embed Veil directly into their own products.

Beyond. Later work extends Veil toward AI agent payments and deeper stablecoin integrations, so that both autonomous software and stable value can move privately on the same rails.

Limitations and Trade-offs

Veil is a serious system, and serious systems have honest limits.

Veil protects the confidentiality of activity inside the shielded pool. It does not erase what happens outside it. The moments where value enters through a deposit and leaves through a withdrawal are the

edges where information can appear, and users who move value carelessly at those edges can reduce their own privacy. Sensible usage matters.

Privacy in a pooled system also grows with participation. A larger and more active shielded pool offers stronger practical privacy than a small one, so the protection each user enjoys improves as the ecosystem and its integrated tokens grow.

The gasless execution model improves usability, but it is a convenience layer, not a change to the trust model. It is designed specifically to avoid introducing custodial risk, and users should understand it as a smoother fee experience rather than a different security guarantee.

Finally, the security story is still being written. Audits are ongoing rather than complete, and the mainnet target of Q3 2026 is a plan, not a settled fact. We would rather state this plainly than overpromise. Cryptographic infrastructure deserves caution, review, and time, and Veil is being built accordingly.

Conclusion

Public blockchains gave the world verifiable money and took away financial privacy in the process. Veil restores that privacy on Robinhood Chain without giving up the verifiability that makes the chain trustworthy. By turning public funds into encrypted private notes, enforcing every action with zero-knowledge proofs, and keeping custody firmly with the user, Veil makes private payments, private commerce, and private finance ordinary rather than exceptional. And because the same shielded architecture is open to the whole ecosystem, privacy stops being a luxury that only a few can build and becomes shared infrastructure that any supported token can offer its holders. That is the layer Robinhood Chain has been missing, and it is the layer Veil is here to provide.