Quero

WHITEPAPER · VERSION 1.0 · NOVEMBER 2026

Own real assets. *Keep* your privacy.

Quero is a market for tokenized real-world assets on Robinhood Chain. It gathers tokenized stocks, ETFs, gold and treasuries from every major issuer into one catalog, prices them with Chainlink, and gives holders privacy that rests on public contracts and zero-knowledge proofs. Users trade from their own wallets. Every contract described in this paper is deployed on Robinhood Chain mainnet (chain ID 4663) at the addresses listed in section 9.

quero.family/whitepaper · official@quero.family

01 Introduction

Tokenized real-world assets are now everyday products. A share of Apple, an S&P 500 fund or an ounce of gold can be held as a token in a wallet the owner controls. The market that grew around them is wide and fragmented. Each issuer has its own token format, its own set of networks and its own venues, so a buyer has to know who issues what, where it trades and how its price is set.

Public ledgers add a second question. Every balance and every order on a transparent chain can be read by anyone who knows the address. For a portfolio of tokenized securities, that means holdings, entry prices and trading intent are open to the whole market.

Quero answers both. It is one market for every issuer, built on Robinhood Chain and priced by Chainlink, with privacy tools that a user can check on chain:

- A catalog that lists each underlying asset once, with every issuer and network that offers it.
- Swap and Bridge with routes from LI.FI across the decentralized exchanges on Robinhood Chain and the bridges into it.
- A Dark Pool where orders stay sealed until the batch closes and cross at the Chainlink price.
- Shield, fixed-denomination pools where a zero-knowledge proof separates a withdrawal from its deposit.
- An anti-quantum wallet whose only key is a hash-based SLH-DSA signature.

02 Markets Live

ASSETS LISTED	ISSUERS	NETWORKS	ON ROBINHOOD CHAIN
1,719	6	9	97

Quero's catalog is built from LI.FI's token lists for nine networks: Robinhood Chain, Ethereum, Solana, Arbitrum, Base, BNB Chain, Optimism, Polygon and Avalanche. Each issuer is recognized by its own naming scheme, the issuer's mark is removed to find the underlying ticker, and every listing of that ticker is grouped under one asset page. On 8 November 2026 the catalog held 1,719 assets: 1,522 stocks, 151 ETFs, 31 treasury products and 15 commodities.

ISSUER	NETWORKS
Robinhood stock tokens	Robinhood Chain
xStocks	Ethereum, Solana, Arbitrum, BNB Chain, Optimism
Ondo Global Markets	Ethereum, Solana, BNB Chain, Arbitrum
Backed	Ethereum, Arbitrum, Base, Polygon, Avalanche, BNB Chain
STOx	Base, Robinhood Chain
Reality	Arbitrum

An asset page shows the asset's price, every issuer that tokenizes it, the networks each issuer uses and the token address on each network. Robinhood stock tokens are read straight from Robinhood Chain: their price comes from the Chainlink feed for that stock, and the value of the tokens outstanding is their supply multiplied by that price. The Oracle feeds page lists every Chainlink feed on Robinhood Chain with its latest answer, heartbeat and update time.

03 Swap and Bridge Live

Swap and Bridge takes a user from what they hold to the asset they want. Quotes come from LI.FI, which compares routes across the decentralized exchanges on Robinhood Chain and across bridges from other networks, including Solana. The interface shows the expected output and the price impact of each route before the wallet asks for a signature.

- Approvals are exact: the wallet approves the amount of the swap.
- Every transaction is simulated first, so a route that would fail is shown as an error before anything is signed.
- Each pool a route passes through charges its own pool fee, paid to that pool's liquidity providers, and gas is paid in Ethereum to Robinhood Chain.

04 Dark Pool Live

MARKETS	COMMIT WINDOW	REVEAL WINDOW	FEE ON A FILL
17	10 min	5 min	0.10%

The Dark Pool crosses buy and sell orders for one tokenized asset against Global Dollar (USDG), between traders, at the Chainlink price. Time is divided into batches of fifteen minutes: a ten-minute commit window followed by a five-minute reveal window. During the commit window an order is only a hash, so its side, size and limit stay private while the batch is open.

1. **Deposit**
   Move the asset or USDG into your balance in the pool. A balance can be topped up at any time, so a deposit stays separate from any order.
2. **Commit**
   Send the hash of your side, amount, limit price and a random salt. The hash also binds the pool, the chain, the batch and your wallet.
3. **Reveal**
   In the reveal window, publish the order behind your hash. The contract checks it against the commitment and sets the amount aside from your balance.
4. **Settle**
   Once the batch ends, any wallet can settle it. The contract reads the Chainlink price, crosses every order whose limit that price meets, and fills the larger side pro rata.
5. **Withdraw**
   Filled amounts and anything that did not cross return to your balance in the pool, ready for the next batch or for withdrawal.

Seventeen markets are open, each against USDG: SPY, QQQ, GLD, SLV, SGOV, AAPL, MSFT, NVDA, AMZN, GOOGL, META, TSLA, AMD, TSM, COIN, PLTR and MSTR. The pool is built for size: an order starts at 1,000 USDG of value at the oracle price. The fee is 0.10% of what a filled order receives and goes to the Quero treasury. Payouts round down and payments round up, with the rounding remainder credited to the treasury, so the contract always holds at least what it owes to its traders.

Window lengths, the fee and the order minimum are immutable values fixed when each pool was deployed, and every pool is open to any wallet.

05 Shield V1 Live

POOLS	PROOF SYSTEM	TREE DEPTH	WHO CAN SHIELD
4	PLONK	20	Any wallet

Shield separates where funds come from and where they go. Each Shield pool accepts one fixed amount: 0.1 Ethereum, 1 Ethereum, 100 USDG or 1,000 USDG. Every deposit in a pool is the same size, so a withdrawal could belong to any of them, and each new deposit widens that set.

1. **Create a note**
   The browser draws two random numbers, a nullifier and a secret. The note that holds them is the key to the deposit and stays with the user.
2. **Shield**
   The deposit sends the pool amount with a commitment, the Poseidon hash of the nullifier and the secret. The pool adds it as a leaf of a Poseidon Merkle tree twenty levels deep.
3. **Prove**
   To withdraw, the browser builds a PLONK proof that the note belongs to one of the pool's leaves, without saying which one, and publishes the hash of the nullifier so the same note can be used once.
4. **Withdraw or swap**
   The pool pays the recipient the user chose, or swaps the amount to USDG or Ethereum in the same transaction through the Uniswap V2 router on Robinhood Chain.

The proof also commits to the withdrawal's parameters: chain, pool, recipient, relayer, fee, swap path, minimum output and deadline. A proof therefore pays exactly the recipient its owner chose. Any wallet can submit it, so a withdrawal can come from a fresh wallet. PLONK uses a universal setup shared across circuits.

Shield V2

Shield V2 extends the pools into a shielded balance: orders on the same pair and side are combined into one swap, each trader's fill settles back into their shielded balance, and tokenized stocks can be held inside Shield, sold back into USDG or withdrawn at any time. Shield V2 is coming soon.

06 Anti-quantum wallet Coming soon

Ordinary wallets sign with ECDSA over secp256k1, a scheme that quantum computers are expected to break. Quero's anti-quantum wallet is an ERC-4337 smart account whose only authority is an SLH-DSA-SHA2-128s signature, the stateless hash-based scheme standardized by NIST as FIPS 205. Its security rests on the SHA-256 hash function, and only the account's SLH-DSA key can move what it holds.

1. **Create**
   The browser generates a 24-word recovery phrase and derives the account's SLH-DSA key from it with HKDF-SHA256. The account address is known before the account is deployed.
2. **Unlock**
   A passkey on the device unlocks an encrypted copy of the key, so day-to-day use takes one passkey touch. The 24 words restore the account on any device.
3. **Sign**
   Each action becomes an ERC-4337 user operation, signed with SLH-DSA in a background worker of the browser.
4. **Submit**
   A relay at relay.quero.family hands the signed operation to the EntryPoint. The signature covers the whole operation, so the relay delivers it exactly as signed.

The account appears as one more choice in Connect, next to the wallets the browser already holds, and works with every Quero feature: Swap, Dark Pool, Shield, portfolio and sign-in. Sign-in accepts the account through ERC-1271, and through ERC-6492 before its first transaction deploys it. The account pays its own gas in Ethereum. The recovery phrase and the key are created and kept in the browser; the relay receives only signed operations.

CONTRACT	ADDRESS
SLH-DSA verifier	0x69dbfB935eA15166b6dCA4BbaD7727A78de0D175
Quantum account factory	0x3437ceF5C0cC67d18F69C5311b44407ACA658e8a
Quantum account implementation	0x339Fc7EaDC5c9349115D36F8CC6defAe17e0DEc4
EntryPoint v0.8	0x4337084D9E255Ff0702461CF8895CE9E3b5Ff108

07 Credit pools

Coming soon

Credit pools let depositors fund loans arranged by approved managers. A pool collects one stablecoin from depositors, who receive ERC-4626 shares. An approved manager lends part of the pool to borrowers, and borrowers repay principal and interest on chain. Every draw and every repayment is a public event, so a pool's book can be read by anyone.

- Interest raises the share price, so depositors earn as loans are repaid.
- Each pool states its borrower profile, target rate, term and reporting in a terms document fixed at creation.
- A share of every pool always stays liquid for withdrawals, at a ratio fixed when the pool is created.
- The manager's fee is a share of interest only, at most 20%, and is fixed when the pool is created.

Quero's credit pool factory is deployed on Robinhood Chain at 0xd880f10e40eF2A6c07C355f61059eDDE8A3744c2. Pools open in the app soon.

08 Prices and oracles

Every price that moves value in Quero comes from Chainlink. The Dark Pool reads a small adapter, ArcaneChainlinkFeed, which combines two Chainlink USD feeds, the asset's feed and the USDG feed, into the price of the asset in USDG base units, scaled by 10^36. For the SPY pool, for example, the adapter reads the RHSPY / USD and USDG / USD feeds.

- The adapter is a fixed contract that reports exactly what Chainlink publishes.

- The adapter accepts only a recent round from each feed, so a batch settles on a current price.

09 Architecture and contracts

Quero's contracts are written in Solidity 0.8.26 on OpenZeppelin 5. The Dark Pool and Shield contracts are deployed without a proxy, and their tokens, fee, windows, minimum and denomination are immutable values set at deployment. Balances in these contracts move only through their owner's own transaction or proof. Funds stay in the user's wallet or in these contracts, and the user signs every transaction.

What you sign

ACTION	TRANSACTIONS
Swap	An exact approval of the input token, then the route call returned by LI.FI.
Dark Pool	Approve and deposit, commit a hash, reveal the order, and withdraw. Settlement can be sent by any wallet.
Shield	Approve (for USDG) and deposit with the commitment. A withdrawal carries the proof and can be sent from any wallet.
Anti-quantum wallet	One SLH-DSA signature per user operation, delivered by the relay to the EntryPoint.

Deployed contracts

CONTRACT	ADDRESS
Dark Pool factory (17 pools)	`0xfC1351f9D303314A96776dA89e70b76f3dAAC14B`
Shield factory	`0x29b98D1B0B564035b32918df077fd33969bcf6c0`
Shield pool, 0.1 Ethereum	`0xfB5F5AA67B61230d16f31a07D03AD68B67dd9F9D`
Shield pool, 1 Ethereum	`0x398D0B62f4b561eb918Fb610ec353506Fd077BE9`
Shield pool, 100 USDG	`0xc43b288839a0A46aCf674DaE0115a0d4dbc9F603`

CONTRACT	ADDRESS
Shield pool, 1,000 USDG	0x6BA0b5EEb90abBBFf5e68083d70Ad39174a0C2ad
Shield PLONK verifier	0x3955DfE3325167bEAe0e69cb94504dfb5B70a00F
Poseidon hasher	0x21Caf566Bc22aC6B424b6eff71051Eb33c6c175E
Credit pool factory	0xd880f10e40eF2A6c07C355f61059eDDE8A3744c2
Quantum account factory	0x3437ceF5C0cC67d18F69C5311b44407ACA658e8a
SLH-DSA verifier	0x69dbfB935eA15166b6dCA4BbaD7727A78de0D175
Global Dollar (USDG)	0x5fc5360D0400a0Fd4f2af552ADD042D716F1d168
QUERO	0x71d85b295653d9C3e7dd2Fc26f26F2c3dB51B2fc

10 The QUERO coin

QUERO is the coin of the Quero project on Robinhood Chain. The values below are read from its contract.

FIELD	VALUE
Name	Quero
Symbol	QUERO
Network	Robinhood Chain (chain ID 4663)
Decimals	18
Total supply	1,000,000,000 QUERO
Contract	0x71d85b295653d9C3e7dd2Fc26f26F2c3dB51B2fc

Holder utility for QUERO is announced on quero.family and in the next edition of this paper.

11 Roadmap

These features are coming soon. Each one opens in the app as it is released.

1. **Shield V2**
   Batched swaps into a shielded balance: hold, buy and sell tokenized assets inside Shield.
2. **Multi-chain buying**
   Buy any listing in the catalog from Quero, on whichever of the nine networks its issuer uses.
3. **Baskets**
   One token backed by a fixed quantity of each component asset, minted by depositing the components and redeemed for them.
4. **Liquidity**
   Every liquidity pool on Robinhood Chain with its exchange, fee tier, depth, volume and estimated fee yield, with deposits from Quero.
5. **Investor verification**
   Verify once with a provider and prove eligibility on chain with a zero-knowledge credential, without revealing identity, country or date of birth.
6. **Issuance**
   Issuers launch permissioned ERC-3643 tokens with compliance rules and an offering document anchored on chain by its hash.

12 Contact

Quero is at quero.family and on X as @querofamily. Questions about this paper: official@quero.family.