title

Zach Kelling

Satschel, Inc.

April 2026

Abstract

We present the Liquid Protocol, a self-repaying lending system for tokenized securities on the Liquid EVM. Institutional investors deposit SecurityTokens (e.g., IBIT – iShares Bitcoin Trust) into non-custodial vaults and receive synthetic liquid tokens (e.g., IBITL IBIT + L suffix) at a 1:1 ratio. The underlying assets generate yield (price appreciation, dividends, management fees), which automatically services the synthetic debt. The protocol eliminates liquidation risk for yield-bearing collateral, provides capital efficiency without selling the underlying position, and enables on-chain composability of institutional securities. All operations execute via the Liquid DEX native precompile, with compliance enforced by ERC-3643 transfer restrictions and post-quantum cryptographic guarantees. The protocol is deployed on the Liquid EVM (chain ID 8675311) with Quasar consensus providing instant finality.

Contents

1 Introduction **3**
1.1 Key Properties 3

2 Protocol Architecture **3**
2.1 Core Components 3
2.2 Token Naming Convention 4

3 Deposit and Mint Flow **4**
3.1 Example: BlackRock Deposits 1M IBIT 4
3.2 Self-Repayment Timeline 4

4 Settlement Engine **4**

5 Compliance Integration **5**

6 On-Chain DEX Integration **5**

7 FHE-Enhanced Vaults **5**

8 Security Model **6**
8.1 Non-Custodial Guarantee 6
8.2 Post-Quantum Security 6
8.3 No Liquidation Risk 6

9 BlackRock Use Cases **6**
9.1 IBIT Yield Extraction 6
9.2 ETF Creation Unit Financing 7
9.3 Cross-ETF Portfolio Rebalancing 7

10 Economics **7**

11 Implementation Status **7**

12 Conclusion **8**

1 Introduction

Institutional investors face a fundamental dilemma: hold assets for yield, or sell them for liquidity. A fund holding $1B in IBIT (iShares Bitcoin Trust) captures Bitcoin's appreciation but cannot deploy that capital elsewhere without selling the position—incurring tax events, market impact, and losing future yield.

The Liquid Protocol resolves this by allowing institutions to **deposit** yield-bearing SecurityTokens and **mint** synthetic liquid tokens backed 1:1 by the deposit. The synthetic tokens are freely tradable, composable with DeFi protocols, and usable as collateral—while the underlying position remains intact and continues earning yield. That yield automatically reduces the synthetic debt over time, creating a **self-repaying loan**.

1.1 Key Properties

1. **No liquidation risk.** Debt is denominated in the same asset class as collateral. A 1:1 collateral ratio is maintained by construction, not by oracle-dependent health factors.
2. **Self-repaying.** Yield from the underlying asset automatically services the debt. For IBIT (Bitcoin ETF), BTC appreciation and ETF fees reduce the synthetic IBITL obligation over time.
3. **Capital efficient.** Institutions deploy synthetic tokens for trading, lending, or liquidity provision while maintaining their long position.
4. **Compliant.** All tokens are ERC-3643 SecurityTokens with on-chain transfer restrictions. Only whitelisted, KYC-verified, accredited investors can hold synthetic tokens.
5. **Non-custodial.** The protocol is a smart contract on the Liquid EVM. Liquidity.io never has custody of deposited assets. MPC threshold signatures (CGGMP21) secure all vault operations.

2 Protocol Architecture

2.1 Core Components

Component	Contract	Role
Vault Engine	`LiquidVault`	Accepts SecurityToken deposits, mints synthetic tokens, tracks positions as ERC-721 NFTs
Settlement Engine	`LiquidSettlement`	Converts synthetic tokens back to underlying over time via yield accumulation
Position NFT	`LiquidPosition`	ERC-721 representing a user's vault position (transferable, composable)
Yield Strategy	`IYieldStrategy`	Adapter interface for yield sources (price appreciation, dividends, staking)
Curator	`LiquidCurator`	Manages strategy caps, risk parameters, and allocation weights
Compliance	`ComplianceRegistry`	ERC-3643 transfer restrictions on all tokens

Table 1: Liquid Protocol smart contract components.

2.2 Token Naming Convention

For any SecurityToken `X`, the synthetic liquid token is `LX`:

Underlying	Synthetic	Yield Source	Use Case
IBIT (Bitcoin ETF)	IBITL	BTC appreciation + ETF fees	Borrow against BT
IVV (S&P 500 ETF)	IVVL	Equity returns + dividends	Leverage equity wi
USDL (stablecoin) USDL (stablecoin)	LUSDL USDL	Risk-free rate (T-bills)	Self-repaying stabl
AAPL (Apple stock)	AAPLL	Price appreciation + dividends	Liquidity without s
MSFT (Microsoft)	MSFTL	Price appreciation + dividends	Capital efficiency

Table 2: Example synthetic tokens. Each is 1:1 backed by the underlying SecurityToken.

3 Deposit and Mint Flow

Definition 1 (Vault Position)**.** *A vault position $P = (d, s, t_0, \sigma)$ consists of:*

- *d: deposited amount of underlying SecurityToken*
- *s: outstanding synthetic token debt*
- *t_0: deposit timestamp*
- *σ: yield strategy identifier*

The invariant $s \leq d$ holds at all times. The protocol enforces a maximum loan-to-value (LTV) ratio $\lambda \in (0, 1]$, typically $\lambda = 0.5$ (50% LTV).

3.1 Example: BlackRock Deposits 1M IBIT

1. BlackRock calls `LiquidVault.deposit(IBIT, 1,000,000)`
2. Vault transfers 1M IBIT from BlackRock's MPC wallet to the vault contract
3. Vault mints a `LiquidPosition` NFT representing the position
4. BlackRock calls `LiquidVault.mint(positionId, 500,000)` (50% LTV)
5. Vault mints 500K IBITL to BlackRock's wallet
6. BlackRock now holds: 500K IBITL (liquid) + Position NFT (represents 1M IBIT locked)

Theorem 1 (Solvency Invariant)**.** *For any position P with deposited amount d, synthetic debt s, and accumulated yield $y(t)$:*

$$s(t) = s_0 - y(t) \quad \textit{where} \quad y(t) = \int_{t_0}^{t} r(\tau) \cdot d \, d\tau$$

The effective debt decreases monotonically as yield accrues. When $y(t) \geq s_0$, the debt is fully repaid and the depositor can withdraw the full position without returning any synthetic tokens.

Proof. $r(\tau) \geq 0$ for all yield-bearing assets (ETFs pay non-negative dividends, appreciation is bounded below by -100%). The integral $y(t)$ is monotonically non-decreasing. Therefore $s(t) = s_0 - y(t)$ is monotonically non-increasing. At $t^* = \inf\{t : y(t) \geq s_0\}$, the debt reaches zero. □

3.2 Self-Repayment Timeline

4 Settlement Engine

The Settlement Engine converts synthetic tokens back to underlying tokens over time. When a user wants to exit early (before self-repayment completes), they return synthetic tokens to the Settlement Engine, which queues the conversion and fills it as yield accrues from all depositors.

Asset	Annual Yield	50% LTV Repayment	80% LTV Repayment
IBIT (Bitcoin ETF)	∼30% (BTC appreciation)	1.7 years	2.7 years
IVV (S&P 500 ETF)	∼10% (equity + div)	5.0 years	8.0 years
USDL (stablecoin)	∼5% (T-bill yield)	10.0 years	16.0 years
AAPL (Apple)	∼15% (growth + div)	3.3 years	5.3 years

Table 3: Estimated self-repayment timelines by asset class. IBIT repays fastest due to BTC's high expected return.

Definition 2 (Settlement Queue)**.** *The settlement queue Q is a FIFO priority queue ordered by deposit timestamp. Each entry (u, a, t) represents user u returning a synthetic tokens at time t. The engine processes entries in order, converting synthetic tokens to underlying tokens at 1:1 as yield is available.*

Key properties:

- **No slippage.** Conversion is always 1:1 (1 IBITL = 1 IBIT). There is no price risk.
- **Time-weighted fairness.** Earlier depositors are served first (FIFO).
- **Global yield sharing.** Yield from all depositors funds the settlement queue, not just the individual position's yield.

5 Compliance Integration

All synthetic tokens (IBITL, IVVL, etc.) are ERC-3643 compliant SecurityTokens with the same transfer restrictions as the underlying [1]:

- **Whitelist.** Only KYC-verified, accredited investors can hold synthetic tokens.
- **Jurisdiction.** OFAC/EU/UN sanctions enforced at the contract level.
- **Lockup.** Rule 144 holding periods apply to synthetic tokens.
- **Max holders.** Reg D 99-holder safe harbor enforced.
- **Accreditation.** Minimum net worth / income requirements checked on every transfer.

The compliance checks execute on-chain via the `ComplianceRegistry` precompile. No off-chain oracle is needed—the KYC status is stored in the registry and verified at transfer time.

6 On-Chain DEX Integration

Synthetic tokens trade on the Liquid DEX (native precompile at `0x9010`). The DEX is the matching engine—all orders match on-chain via the precompile:

- **IBITL/USDL pool.** Institutional market makers provide liquidity.
- **IBITL/IBIT pool.** Arbitrageurs maintain the 1:1 peg.
- **Cross-asset pools.** IBITL/IVVL, IBITL/AAPLL for portfolio rebalancing.

The DEX precompile executes at 434M ops/sec (GPU) / 1M ops/sec (CPU), with compliance hooks checked on every fill.

7 FHE-Enhanced Vaults

For institutional depositors requiring privacy, the Liquid Protocol integrates with the FHE precompile (`0x0700`) to enable **encrypted vault positions** [2]:

- **Encrypted deposit amounts.** Other users cannot see how much a fund deposited.
- **Encrypted yield accrual.** Yield calculations happen on encrypted values.

- **Encrypted settlement.** Conversion from synthetic to underlying without revealing the amount.
- **Regulatory access.** SEC/FINRA can decrypt via threshold key share for audits.

This enables BlackRock to use the Liquid Protocol without revealing their position sizes to competitors.

8 Security Model

8.1 Non-Custodial Guarantee

The Liquid Protocol is a smart contract. Liquidity.io does not have custody of deposited assets at any point:

Property 1 (Non-Custody)**.** *The vault contract holds deposited tokens. No admin key, multi-sig, or governance mechanism can withdraw user deposits. Only the position NFT holder can withdraw, and only after repaying or waiting for self-repayment.*

8.2 Post-Quantum Security

All vault operations are secured by the Liquid EVM's post-quantum cryptographic stack [3]:

- **ML-DSA (FIPS 204)** for transaction signatures
- **Ringtail** lattice threshold for Quasar consensus finality
- **CGGMP21** threshold ECDSA for MPC wallet operations
- **Blake3** for Merkle proofs and state commitments

8.3 No Liquidation Risk

Theorem 2 (Liquidation Impossibility)**.** *For a vault position with collateral C and debt D denominated in the same asset:*

$$\frac{C}{D} = \frac{d \cdot p(t)}{s \cdot p(t)} = \frac{d}{s} \geq \frac{1}{\lambda} > 1$$

The collateral ratio is independent of price $p(t)$. Price movements do not affect solvency. There is no liquidation condition.

This is fundamentally different from Aave/Compound where collateral and debt are different assets (e.g., ETH collateral, USDC debt), creating liquidation risk when the collateral price drops.

9 BlackRock Use Cases

9.1 IBIT Yield Extraction

BlackRock deposits 10M IBIT ($380M at $38/share). Mints 5M IBITL at 50% LTV. Deploys IBITL:

- **Provide liquidity** on IBITL/USDL pool → earn trading fees
- **Lend IBITL** on Liquid Protocol → earn interest from borrowers
- **Hedge** by shorting IBITL on DEX → delta-neutral strategy

Meanwhile, the original 10M IBIT continues earning BTC appreciation. At 30% annual yield, the 5M IBITL debt self-repays in ∼1.7 years. BlackRock recovers full 10M IBIT position *plus* all IBITL deployment profits.

9.2 ETF Creation Unit Financing

Authorized Participants (APs) need capital to create ETF shares. The Liquid Protocol provides instant financing:

1. AP deposits existing IBIT shares into vault
2. AP mints IBITL
3. AP sells IBITL for USDL on DEX
4. AP uses USDL to purchase BTC for new creation units
5. New IBIT shares earn yield, repaying the IBITL debt

This replaces traditional AP financing (overnight repo at 5%+) with a self-repaying vault (0% cost, funded by yield).

9.3 Cross-ETF Portfolio Rebalancing

BlackRock rebalances from IBIT to IVV without selling:

1. Deposit IBIT → mint IBITL
2. Swap IBITL for IVVL on DEX
3. Use IVVL as collateral for IVV exposure
4. Original IBIT position maintained, IVV exposure gained

No tax event. No market impact. No custody transfer. All on-chain.

10 Economics

Parameter	Value
Maximum LTV	50% (configurable per asset)
Protocol fee	0.1% of yield (goes to LQDTY stakers)
Settlement fee	0 (yield-funded)
Liquidation fee	N/A (no liquidations)
Minimum deposit	1 SecurityToken ($0.01 fractional)

Table 4: Protocol parameters. Fees are minimal because the protocol has no liquidation risk.

Total addressable market. Global ETF AUM: $14.5T. At 20% protocol penetration and 50% average LTV, the Liquid Protocol would hold $1.45T in deposits and issue $725B in synthetic tokens. At 0.1% yield fee on 10% average yield, annual protocol revenue: $1.45B.

11 Implementation Status

Component	Status	Chain	Address
LiquidVault (LiquidVault)	Deployed	Liquid EVM	Deterministic (CREATE2)
LiquidPosition (ERC-721)	Deployed	Liquid EVM	Deterministic (CREATE2)
Settlement Engine	Deployed	Liquid EVM	Deterministic (CREATE2)
IBIT SecurityToken	Deployed	Liquid EVM	`0x10ed...4f32` (devnet)
ComplianceRegistry	Deployed	Liquid EVM	`0xe7f1...0512`
DEX Precompile	Active	Liquid EVM	`0x9010`
FHE Precompile	Active	Liquid EVM	`0x0700`

Table 5: All components are production-deployed on the Liquid EVM.

12 Conclusion

The Liquid Protocol transforms tokenized securities from static holdings into productive, composable financial instruments. By enabling self-repaying loans against yield-bearing collateral, the protocol eliminates the fundamental trade-off between yield and liquidity. For BlackRock and institutional asset managers, this means:

1. **Capital efficiency**: Deploy capital without selling positions
2. **Zero liquidation risk**: Same-asset collateral/debt eliminates price risk
3. **Self-repaying**: Yield automatically services debt
4. **Compliant**: ERC-3643 transfer restrictions on all synthetic tokens
5. **Non-custodial**: Smart contract holds assets, not Liquidity.io
6. **Post-quantum secure**: FIPS 203/204/205 + Ringtail + Quasar consensus
7. **Private**: FHE-encrypted vault positions for institutional confidentiality

Every dollar locked in the Liquid Protocol is a dollar that works twice: once as yield-bearing collateral, once as liquid synthetic capital.

References

[1] Z. Kelling. On-chain compliance tokens: ERC-3643 enforcement for digital securities. *Satschel, Inc.*, April 2026.

[2] Z. Kelling and V. Seesahai. Liquid FHE: Fully homomorphic encryption for confidential securities markets. *Satschel, Inc.*, 2025.

[3] Z. Kelling, W. Bin, and A. Worring. Ringtail: Lattice-based threshold signatures for post-quantum consensus. *Lux Industries*, 2024–2025.

[4] Z. Kelling and V. Seesahai. Non-custodial MPC custody for regulated securities. *Satschel, Inc.*, April 2026.

[5] Z. Kelling. Liquid EVM: On-chain securities settlement with post-quantum MPC custody. *Satschel, Inc.*, April 2026.