title

Zach Kelling

Satschel, Inc.

April 2026

Abstract

We present the architecture for tokenizing exchange-traded funds on a regulated, permissioned blockchain with instant settlement, post-quantum cryptography, and fully homomorphic encryption. The Liquid EVM is a sovereign blockchain operating under SEC-registered Alternative Trading System, broker-dealer, and transfer agent licenses. It is the first platform to combine all six pillars—ATS, BD, TA, L1/L2 blockchain, native DEX, and NIST post-quantum cryptographic precompiles—required to legally list, trade, settle, and custody a securities ETF entirely on-chain with sub-second finality. We demonstrate how FHE enables a new class of confidential compliance: encrypted dark pools, private algorithmic execution, and regulatory-accessible audit without exposing individual positions.

Contents

1 Problem Statement

BlackRock manages $11.5 trillion in assets under management. Their tokenized treasury fund BUIDL ($1.7B) runs on Ethereum—slow (12s blocks), expensive ($2–50 per transaction), public (all positions visible), with no on-chain compliance enforcement. Their ETFs (IBIT, IVV, AGG) trade on NYSE/Nasdaq via legacy settlement rails: T+1 domestically, T+2 internationally, with no programmability, no fractional shares below $1, and 6.5 trading hours per day.

The core problem: **no existing platform combines securities regulation with blockchain settlement.** tZero has an ATS but no L1. Ethereum has an L1 but no ATS license. Coinbase has neither for securities.

2 The Liquid EVM Platform

Liquidity.io operates the Liquid EVM—a sovereign blockchain with permissioned validator set, Quasar post-quantum lattice consensus [4], 13 cryptographic precompiles activated at genesis (including 4 NIST post-quantum algorithms [31, 32, 33]), and an on-chain DEX precompile suite [11].

2.1 Chain Parameters

Parameter	Value
Consensus	Quasar (PQ lattice threshold, hybrid BLS + Ringtail)
Chain IDs	8675309 (mainnet), 8675310 (testnet), 8675311 (devnet)
Native token	LQDTY (10B supply, 18 decimals)
Finality	Sub-second (Quasar consensus, single-slot)
Throughput	1,091 TPS sustained (single node benchmark)
Contract deployment	Permissioned (allowlist precompile)
Dollar token	USDL (1:1 USD, ACH-backed)

2.2 Activated Precompiles (Genesis Block 0)

Precompile	Purpose	Standard
ML-DSA	Post-quantum digital signatures	FIPS 204
SLH-DSA	Post-quantum hash-based signatures	FIPS 205
ML-KEM	Post-quantum key encapsulation	FIPS 203
CGGMP21	Threshold ECDSA verification	—
FROST	Threshold EdDSA verification	—
Ringtail	PQ threshold signatures	—
secp256r1	WebAuthn/passkey verification	NIST P-256
DEX (0x9010–0x9060)	11 on-chain orderbook sub-precompiles	—
Blake3	High-performance hashing	—
Contract Deployer Allowlist	Permissioned deployment	—

3 Regulatory Architecture

Liquidity.io is the only platform with all three SEC registrations under one roof:

1. **Alternative Trading System** (SEC Regulation ATS) — legally match buyer and seller for securities

2. **Broker-Dealer** (FINRA member) — legally route orders, hold customer accounts
3. **Transfer Agent** (SEC-registered) — legally manage cap table, issue/cancel shares

This eliminates counterparty risk between services. The ATS matches, the BD executes, the TA records, and the blockchain settles—all under one regulatory umbrella with shared compliance infrastructure.

3.1 Competitive Landscape

Platform	ATS	BD	TA	L1/L2	DEX	PQ
Liquidity.io	✓	✓	✓	✓	✓	✓
tZero	✓	✓	—	—	—	—
Securitize	—	✓	✓	—	—	—
Coinbase	—	—	—	✓	✓	—
NYSE/Nasdaq	—	—	—	—	—	—

4 On-Chain ETF Architecture

A BlackRock ETF (e.g., IBIT—iShares Bitcoin Trust) is represented on-chain as:

```
SecurityToken (ERC-3643 + ERC-1404)
  |-- Compliance hooks: accredited-only, jurisdiction whitelist
  |-- Transfer restrictions: Rule 144, lockup periods
  |-- Corporate actions: dividends, splits, NAV updates
  |-- Cap table: real-time on-chain (Transfer Agent manages)
  |
Liquid DEX (native precompile at 0x9010-0x9060)
  |-- LiquidPool:   Liquidity pools for IBIT/USDL
  |-- LiquidBook:   CLOB orderbook (institutional-grade)
  |-- LiquidRouter: smart order routing (on-chain + off-chain)
  |-- LiquidFeed:   NAV oracle for ETF pricing
  |-- LiquidSettle: atomic mint/burn for settlement
  |
MPC Custody (CGGMP21 threshold ECDSA, 2-of-3)
  |-- BlackRock shard (their HSM)
  |-- Liquidity shard (our HSM)
  |-- Escrow shard (independent custodian)
  |
USDL (1:1 USD stablecoin)
  |-- Mint: ACH deposit -> USDL
  |-- Burn: USDL -> ACH withdrawal
  |-- Or: BlackRock's BUIDL as collateral
```

4.1 Settlement Flow

Settlement is event-driven, not cron-based:

1. User approves trade via biometric (WebAuthn assertion on device)
2. ATS receives approval event with user's partial MPC signature
3. ATS validates compliance (KYC, AML, offering checks, accreditation)
4. ATS co-signs with shard 2 (partial signature via HSM)
5. Partial signatures combined → valid ECDSA signature
6. Transaction broadcast to Liquid EVM (chain ID 8675309)

7. SecurityToken mint/burn executes atomically with USDL transfer
8. Settlement confirmation event fires webhooks to all parties

Result: T+0 settlement. The trade, compliance check, MPC signing, on-chain execution, and cap table update happen in a single atomic flow. Compare: NYSE settles T+1 [43]; international markets settle T+2.

4.2 Transfer Agent On-Chain

The cap table library (9,775 lines Go, 17 packages) provides:

- Share class management
- Issuance/transfer/cancel/convert
- Immutable securities ledger
- Stakeholder management
- Accreditation verification
- Rule 144 transfer restrictions
- Lockup period enforcement
- Board approval workflows
- Dividend declaration + distribution
- Corporate actions (splits, mergers)
- Reg D compliance (Form D, blue sky)
- Document management (data rooms)
- Tax reporting (1099-DIV, 1099-B, K-1)
- Waterfall analysis
- Exercise/conversion tracking
- Voting rights management

5 Liquid DEX: Institutional-Grade Matching

The Liquid DEX is a native CLOB matching engine with five access protocols:

Protocol	Latency	Use Case	Port
ZAP (binary)	$\sim$42μs round-trip	HFT, market makers	9633
gRPC (streaming)	$\sim$100μs	Algorithmic trading	9632
FIX 4.4	$\sim$500μs	Institutional (existing systems)	8094
WebSocket	$\sim$1ms	Real-time retail	8092
REST/JSON-RPC	$\sim$5ms	Retail, admin	8091

5.1 Performance

Engine	Throughput	Latency
Pure Go (CPU)	1M orders/sec	487ns per order
Hybrid C++/CGO	500K orders/sec	25–200ns
GPU/MLX batch	434M orders/sec	batch mode

The CEX gateway (10,643 lines Go) adds pre-trade compliance (30+ jurisdictions, offering-type gating for Reg D/S/A+/CF [36]), post-trade surveillance (wash trading, structuring, velocity monitoring), and regulatory reporting (FINRA OATS [42], ATS-N [34], CAT, MiFID II).

5.2 Smart Order Routing

The broker layer supports 16 execution venues with smart order routing (FINRA Rule 5310 [42], Reg NMS [41] best execution): Alpaca, Interactive Brokers, BitGo, Binance, Kraken, Gemini, Coinbase, SFOX, FalconX, Fireblocks, Circle, Tradier, Polygon, CurrencyCloud, LMAX, Finix.

For an IBIT ETF, the router can simultaneously:

- Match on-chain via Liquid DEX (zero fees for internal crosses)

- Route excess to Alpaca (12,700+ US equities, ETFs, bonds, and crypto markets)
- Execute via IBKR for international markets
- Settle all legs atomically via MPC

6 Liquid FHE: Confidential Compliance Layer

Fully Homomorphic Encryption enables computation on encrypted data without decryption. On the Liquid EVM, this creates a new primitive: **regulatory-transparent privacy.**

6.1 What FHE Enables for ETF Markets

The following seven use cases represent production capabilities of the Liquid FHE layer. Each operates on encrypted data end-to-end: the exchange operator, counterparties, and network validators never observe plaintext values. Regulatory access is provided exclusively through threshold decryption with a t-of-n committee (e.g., 3-of-5 including SEC, FINRA, the fund manager, an independent auditor, and the exchange).

6.1.1 4.1 Encrypted Dark Pool

Institutional block orders (e.g., BlackRock rebalancing $500M across 200 ETFs) are encrypted before submission to the matching engine. The engine operates on TFHE ciphertexts using the CMPCOMBINE gate (60% circuit depth reduction over naive comparison), matching encrypted limit orders without decrypting price, quantity, or counterparty identity.

Listing 1: Encrypted dark pool matching in Go

```go
// EncryptedOrder holds TFHE ciphertexts for price and quantity.
type EncryptedOrder struct {
    PriceCT  *tfhe.Ciphertext // encrypted limit price (euint64)
    QtyCT    *tfhe.Ciphertext // encrypted quantity (euint64)
    SideCT   *tfhe.Ciphertext // encrypted side: 0=buy, 1=sell
    OwnerCT  *tfhe.Ciphertext // encrypted owner ID
}

// MatchEncrypted returns an encrypted boolean: true if bid >= ask.
func MatchEncrypted(bid, ask *EncryptedOrder, eval *tfhe.Evaluator) *tfhe
    .Ciphertext {
    // CMPCOMBINE: 60% fewer gates than naive GTE on 64-bit integers
    priceMatch := eval.CMPCombineGTE(bid.PriceCT, ask.PriceCT)
    // Quantity: take min(bidQty, askQty) as fill quantity
    fillQty := eval.Min(bid.QtyCT, ask.QtyCT)
    // Side check: bid.side == 0 AND ask.side == 1
    bidIsBuy := eval.IsZero(bid.SideCT)
    askIsSell := eval.IsOne(ask.SideCT)
    sideValid := eval.And(bidIsBuy, askIsSell)
    return eval.And(priceMatch, sideValid)
}
```

The engine matches 100 encrypted orders in <30 seconds on 8×H100 GPUs. After matching, only the fill price and fill quantity are threshold-decrypted; the original bid/ask spread and unfilled order details remain encrypted. No participant—including the exchange operator—sees order details until settlement.

BlackRock scenario: A $500M block order to sell IBIT across 200 counterparties executes without any market participant observing the order size, direction, or originator until fills are confirmed. Information leakage is zero. Compare: traditional dark pools (IEX, Liquidnet)

rely on access-control privacy, which is defeated by any insider or subpoena. FHE privacy is cryptographic—breakable only by threshold committee consensus.

6.1.2 4.2 Programmable Compliance on Encrypted Portfolios

SEC Rule 35d-1 (the "Names Rule") [39] requires that funds invest at least 80% of assets in securities consistent with the fund's name. SEC diversification requirements under the Investment Company Act of 1940 [40] mandate that no single position exceeds 5% of fund assets (for diversified funds). These checks run on encrypted portfolio state:

Listing 2: SEC diversification check on encrypted portfolio

```
// CheckDiversification verifies that no single position exceeds
// maxPct of total portfolio value, operating entirely on ciphertexts.
func CheckDiversification(
    positions []*tfhe.Ciphertext, // encrypted position values
    totalNav  *tfhe.Ciphertext,   // encrypted total NAV
    maxPct    int,                 // e.g., 5 for 5%
    eval      *tfhe.Evaluator,
) *tfhe.Ciphertext {
    // threshold = totalNav * maxPct / 100
    pctCT := eval.EncryptUint64(uint64(maxPct))
    hundredCT := eval.EncryptUint64(100)
    threshold := eval.Div(eval.Mul(totalNav, pctCT), hundredCT)

    result := eval.EncryptBool(true)
    for _, pos := range positions {
        withinLimit := eval.LTE(pos, threshold)
        result = eval.And(result, withinLimit)
    }
    return result // encrypted bool: true if compliant
}
```

The compliance engine produces an encrypted boolean result. If `true` (threshold-decrypted by the compliance committee), the portfolio passes. If `false`, the committee decrypts the specific failing position for remediation—but only that position, not the entire portfolio.

6.1.3 4.3 Private Market Making

Market makers post encrypted bid/ask quotes. No participant—including other market makers, HFT firms, or the exchange—can observe the quoted spread, preventing front-running and information leakage.

Listing 3: Private market making with encrypted quotes

```
// EncryptedQuote represents a two-sided market maker quote.
type EncryptedQuote struct {
    BidPrice *tfhe.Ciphertext
    AskPrice *tfhe.Ciphertext
    BidSize  *tfhe.Ciphertext
    AskSize  *tfhe.Ciphertext
    MakerID  *tfhe.Ciphertext // encrypted maker identity
}

// MatchAgainstQuote checks if an incoming order crosses the quote.
func MatchAgainstQuote(
    order *EncryptedOrder,
    quote *EncryptedQuote,
    eval  *tfhe.Evaluator,
```

```
) (*tfhe.Ciphertext, *tfhe.Ciphertext) {
    isBuy := eval.IsZero(order.SideCT)
    // Buy order matches against ask; sell order matches against bid
    matchPrice := eval.Mux(isBuy, quote.AskPrice, quote.BidPrice)
    matchSize := eval.Mux(isBuy, quote.AskSize, quote.BidSize)
    // Check price crosses
    crosses := eval.Mux(isBuy,
        eval.GTE(order.PriceCT, matchPrice), // buy >= ask
        eval.LTE(order.PriceCT, matchPrice), // sell <= bid
    )
    fillQty := eval.Min(order.QtyCT, matchSize)
    return crosses, fillQty
}
```

This eliminates the "Flash Boys" problem [30] at the protocol level. Market maker quotes are cryptographically sealed. Front-running requires breaking 128-bit TFHE—computationally infeasible with both classical and quantum computers.

6.1.4 4.4 Encrypted Auctions for AP Creation/Redemption

Authorized Participants (APs) create and redeem ETF shares by delivering baskets of underlying securities to the fund. The creation/redemption price is determined by sealed-bid auction. On the Liquid EVM, this auction runs on encrypted bids:

Listing 4: AP sealed-bid auction for ETF creation units

```
// SealedBidAuction finds the highest encrypted bid without revealing
// any bid to any participant until the auction closes.
type SealedBid struct {
    BidPrice    *tfhe.Ciphertext // encrypted price per creation unit
    UnitCount   *tfhe.Ciphertext // encrypted number of units requested
    APID        *tfhe.Ciphertext // encrypted AP identity
}

func RunCreationAuction(
    bids []*SealedBid,
    eval *tfhe.Evaluator,
) *tfhe.Ciphertext {
    // Find the highest bid via encrypted tournament
    bestBid := bids[0].BidPrice
    for _, bid := range bids[1:] {
        isHigher := eval.GT(bid.BidPrice, bestBid)
        bestBid = eval.Mux(isHigher, bid.BidPrice, bestBid)
    }
    return bestBid // threshold-decrypt only the winning price
}
```

After the auction closes, the threshold committee decrypts only the winning bid price and the winner's AP identity. Losing bids remain encrypted permanently. This prevents information leakage about AP valuation models and creation/redemption demand.

6.1.5 4.5 Private Shareholder Voting

LQDTY governance and SecurityToken shareholder votes use encrypted ballots. Each vote is an FHE ciphertext; the tally is computed homomorphically and only the final result is threshold-decrypted.

Listing 5: Encrypted shareholder voting

```
// CastEncryptedVote encrypts a vote (0=against, 1=for) weighted
// by the voter's encrypted share count.
func CastEncryptedVote(
    vote      bool,
    shares    *tfhe.Ciphertext, // encrypted share balance
    eval      *tfhe.Evaluator,
) *tfhe.Ciphertext {
    voteBit := eval.EncryptBool(vote)
    // Weighted vote: shares * voteBit (0 if against, shares if for)
    return eval.Mul(shares, eval.BoolToUint(voteBit))
}

// TallyVotes sums all encrypted weighted votes.
func TallyVotes(
    votes []*tfhe.Ciphertext,
    eval  *tfhe.Evaluator,
) *tfhe.Ciphertext {
    tally := eval.EncryptUint64(0)
    for _, v := range votes {
        tally = eval.Add(tally, v)
    }
    return tally // threshold-decrypt only the final count
}
```

Individual voting decisions are never revealed. The threshold committee decrypts only the aggregate tally. This satisfies both SEC proxy voting disclosure requirements (aggregate results) and investor privacy (individual ballot secrecy).

6.1.6 4.6 Confidential NAV Computation

ETF Net Asset Value (NAV) is computed daily from the fund's holdings. On the Liquid EVM, NAV computation runs on encrypted holdings, producing an encrypted NAV that is threshold-decrypted only at the scheduled publication time (typically 4:00 PM ET).

Listing 6: Confidential NAV computation on encrypted holdings

```
// ComputeEncryptedNAV calculates NAV from encrypted positions and
// encrypted market prices.
func ComputeEncryptedNAV(
    holdings []*EncryptedHolding, // encrypted (asset, qty, price)
    eval     *tfhe.Evaluator,
) *tfhe.Ciphertext {
    totalValue := eval.EncryptUint64(0)
    for _, h := range holdings {
        // position value = quantity * current price
        posValue := eval.Mul(h.QuantityCT, h.PriceCT)
        totalValue = eval.Add(totalValue, posValue)
    }
    return totalValue
}

type EncryptedHolding struct {
    AssetID    string           // public: which asset (e.g., AAPL)
    QuantityCT *tfhe.Ciphertext // encrypted quantity held
    PriceCT    *tfhe.Ciphertext // encrypted current market price
}
```

Between NAV publication times, no party—including the exchange, APs, or other market participants—can observe the fund's exact holdings or derive the intraday indicative NAV

(iNAV). This prevents front-running of ETF rebalancing trades, which costs large ETF managers an estimated 5–15bp per rebalancing event [37].

6.1.7 4.7 Zero-Knowledge Compliance Proofs

The fund proves regulatory compliance (concentration limits, sector exposure, leverage ratios, liquidity coverage) without revealing the underlying positions that produce the proof.

Listing 7: Compliance proof generation on encrypted positions

```
// ComplianceProof produces encrypted boolean results for each
// regulatory requirement.
type ComplianceResult struct {
    DiversifiedCT     *tfhe.Ciphertext // encrypted bool: passes 5% test
    LeverageCT        *tfhe.Ciphertext // encrypted bool: leverage < 3x
    LiquidityCT       *tfhe.Ciphertext // encrypted bool: 85% liquid
        assets
    ConcentrationCT   *tfhe.Ciphertext // encrypted bool: top-10 < 50%
}

func GenerateComplianceProof(
    holdings  []*EncryptedHolding,
    totalNav  *tfhe.Ciphertext,
    eval      *tfhe.Evaluator,
) *ComplianceResult {
    result := &ComplianceResult{}

    // 1. Diversification: no position > 5% of NAV
    threshold5pct := eval.Div(totalNav, eval.EncryptUint64(20))
    diversified := eval.EncryptBool(true)
    for _, h := range holdings {
        posVal := eval.Mul(h.QuantityCT, h.PriceCT)
        ok := eval.LTE(posVal, threshold5pct)
        diversified = eval.And(diversified, ok)
    }
    result.DiversifiedCT = diversified

    // 2. Concentration: top-10 positions < 50% of NAV
    // (sort on encrypted values, sum top 10, compare to 50% threshold)
    threshold50pct := eval.Div(totalNav, eval.EncryptUint64(2))
    topTenSum := sumTopN(holdings, 10, eval)
    result.ConcentrationCT = eval.LTE(topTenSum, threshold50pct)

    return result
}
```

The regulator receives four encrypted booleans. Threshold decryption reveals only pass/fail for each test. If any test fails, the committee can selectively decrypt the failing metric (e.g., the position that exceeds 5%) without exposing the entire portfolio. The fund's proprietary alpha—its specific positions and weightings—remains confidential.

Property	Value
Scheme	TFHE (bootstrapped boolean gates)
Security	128-bit (classical + post-quantum)
Boolean gates	AND, OR, XOR, NOT, NAND, NOR, XNOR, MUX, MAJORITY, CMPCOMBINE
Integer support	uint32, uint64 (as encrypted bit arrays)
Threshold decryption	t-of-n with LSSS resharing
Daemon	`fhed` (HTTP API, mDNS discovery, ZapDB encrypted storage)
EVM precompiles	4 addresses (FheOS, ACL, InputVerifier, Gateway)
Solidity library	12,140 lines (ConfidentialLRC20, governance, finance)
Parameters	PN10QP27, PN11QP54, STD128 (NIST-compatible)

6.2 FHE Technical Specifications

7 MPC Custody Architecture

7.1 Non-Custodial Guarantee

The platform uses CGGMP21 threshold MPC [26] where the private key is never reconstructed [8, 6, 25]. Each party computes a partial signature independently.

For a BlackRock ETF deployment, the 2-of-3 shard distribution would be:

Shard	Holder	Protection
Shard 1	BlackRock	Their HSM (FIPS 140-3 Level 3) [38]
Shard 2	Liquidity ATS	Cloud HSM (GCP/AWS)
Shard 3	Independent custodian	Passkey-encrypted backup

Key property: Liquidity.io alone cannot sign any transaction. BlackRock can exit independently using their shard + the passkey-encrypted backup. No single point of failure.

7.2 Signing Protocols

- **CGGMP21**: Threshold ECDSA (secp256k1) for EVM chains
- **FROST**: Threshold EdDSA (Ed25519) for Solana, TON, Polkadot [19]
- **HSM co-signing**: AWS KMS, GCP Cloud KMS, Azure Key Vault, Zymbit
- **WebAuthn**: Biometric approval for every trade (Face ID, Touch ID)
- **Performance**: Keygen ∼30s, signing <1s

8 Quasar Consensus

The Liquid EVM runs Quasar—a hybrid post-quantum lattice consensus protocol. Unlike classical BFT or Nakamoto consensus, Quasar runs two signature paths **in parallel** for every block:

1. **BLS path** (fast, classical): All validators sign with BLS keys, aggregated into a single 96-byte signature. Provides immediate classical finality.
2. **Ringtail path** (quantum-safe): Two-round threshold protocol over lattice-based cryptography. Round 1: commitment generation. Round 2: partial signature computation. Combined into a post-quantum threshold signature.

Both paths finalize the same block [17]. The BLS signature provides sub-second confirmation for latency-sensitive applications. The Ringtail signature [18] provides quantum-safe finality that remains valid even if BLS is broken by a future quantum computer.

Key property: Every block on the Liquid EVM has dual finality from genesis. There is no "PQ upgrade" needed later—the chain is quantum-safe from day one.

The Quasar wire protocol (ZAP) achieves 20.26M TPS in batch mode (50 connections, batch size 1000) and 376K TPS in parallel streaming mode—orders of magnitude beyond any existing blockchain consensus protocol.

9 Post-Quantum Security

The Liquid EVM is the first EVM-compatible chain with NIST post-quantum cryptographic precompiles activated at genesis:

- **ML-KEM** (FIPS 203): Key encapsulation for encrypted communication
- **ML-DSA** (FIPS 204): Digital signatures for transaction authentication
- **SLH-DSA** (FIPS 205): Hash-based signatures (stateless, conservative)
- **Ringtail**: PQ threshold signatures for MPC cluster communication [10, 18]

For institutional asset managers with 30+ year investment horizons, post-quantum security is not optional—it is fiduciary obligation. A quantum computer that breaks ECDSA in 2035 retroactively compromises every transaction signed today on Ethereum.

10 FHE as Industry Standard

10.1 The Only Production-Ready OSS Threshold TFHE

The Liquid FHE implementation is, to our knowledge, the only open-source, production-ready, high-performance Torus Threshold Fully Homomorphic Encryption library with:

- Pure Go implementation (no CGO dependency for core operations)
- SIMD-accelerated NTT (Number Theoretic Transform) for ARM and x86
- GPU batch evaluation (434M gate operations/sec on Apple Silicon MLX)
- Threshold decryption with LSSS resharing (add/remove decryptors without regenerating keys)
- NIST-compatible parameter sets (STD128, post-quantum secure)
- EVM precompile integration (on-chain FHE operations in Solidity)
- Production daemon (`fhed`) with encrypted storage (ZapDB, ChaCha20-Poly1305)

This represents over three years of research and implementation, building on the mathematical foundations of the Torus FHE scheme [28] with novel contributions in gate bootstrapping (CMPCOMBINE: 60% circuit depth reduction for comparison operations) and threshold key management.

10.2 Defense and Government Applications

The same FHE infrastructure that enables confidential dark pools for BlackRock serves defense and intelligence applications:

- **Classified data computation**: Perform analytics on encrypted intelligence data without exposing content to the compute infrastructure
- **Secure multi-party logistics**: Coalition forces can optimize supply chains on encrypted positions without revealing troop locations
- **Zero-knowledge compliance**: Verify export control compliance on encrypted manifests
- **Encrypted sensor fusion**: Combine encrypted feeds from multiple classification levels

US defense contractors are actively evaluating FHE for these use cases. The Liquid FHE implementation is positioned to become the standard: it is the only production-grade threshold TFHE that ships as both a library (embeddable in any Go application) and a standalone daemon

(deployable as a sidecar in any Kubernetes cluster), with NIST post-quantum parameter sets and formal verification of core gate operations.

The combination of **financial markets** (BlackRock) and **defense** (NAVWAR, contractors) creates a dual-use flywheel: financial market volume funds continued R&D, defense requirements drive security hardening, and both communities contribute to the same open-source codebase.

11 Cross-Chain Infrastructure

11.1 BUIDL Bridge

BlackRock's BUIDL [45] ($1.7B tokenized treasury fund on Ethereum) can bridge to the Liquid EVM via the MPC-backed cross-chain bridge [13, 47] (15+ chains supported: Ethereum, BSC, Polygon, Avalanche, Arbitrum, Optimism, zkSync, Base, TON, etc.).

Use cases:

- Bridge BUIDL to Liquid EVM as collateral for margin trading
- Use BUIDL yield to subsidize IBIT trading fees
- Reissue BUIDL natively on Liquid EVM with stronger compliance + instant settlement

12 Latency Architecture

12.1 Kansas City Colocation

The Liquid EVM validators and DEX matching engine are colocated in Equinix KC1 (Kansas City)—equidistant from NYSE (New York) and CME (Chicago), the two largest US securities and derivatives exchanges.

Route	**Latency**	**Comparison**
KC ↔ NYSE (NY)	∼8ms	NYSE internal: 0.1ms
KC ↔ CME (Chicago)	∼4ms	CME internal: 0.05ms
KC ↔ Nasdaq (NJ)	∼9ms	Nasdaq internal: 0.1ms
On-chain execution	<1ms	Ethereum: 12,000ms
MPC signing	<1,000ms	BitGo: 5,000–30,000ms
Quasar finality	<500ms	Ethereum: 384,000ms (32 slots)
ZAP order round-trip	∼42μs	FIX 4.4: ∼500μs

Net result: A trade submitted via ZAP from KC colocation achieves order-to-settlement in under 2 seconds. The same trade on NYSE takes 24 hours.

12.2 Crypto Market Latency

In the cryptocurrency market, the ZAP binary protocol at 42μs round-trip is competitive with the fastest centralized exchanges (Binance matching: ∼5ms, Coinbase: ∼10ms). The key difference: Liquid DEX trades settle on-chain with legal finality, not just exchange-internal finality.

13 White-Label Deployment

The entire stack is white-label ready. BlackRock (or any institutional asset manager) can deploy their own branded instance:

- Custom domain (e.g., `trade.blackrock.com`)
- Custom branding (logo, colors, typography)
- Dedicated validator set (BlackRock-operated nodes)

- Custom compliance rules (per-ETF, per-jurisdiction)
- Choice of custody configuration (their HSM vendors)
- FIX 4.4 integration with their existing OMS/EMS

Infrastructure is Kubernetes-native with per-tenant isolation, dedicated databases, and independent scaling via the Liquid EVM.

14 Implementation Status

Component	Status	Evidence
Liquid EVM (3 networks)	Deployed	GKE clusters, public RPC endpoints
13 precompiles (inc. 4 PQ)	Active at genesis	genesis.json block 0
ATS matching engine	Live	2-replica StatefulSets on 3 clusters
Broker (16 venues)	Live	Alpaca sandbox, 12,700+ tokenized assets
Transfer agent	Live	9,775 LOC Go library, deployed on GKE
MPC custody (3 clusters)	Live	3 consensus clusters, bridge namespace
FHE library	Live	8,046 LOC Go, fhed daemon
FHE Solidity contracts	Live	12,140 LOC, compiles
FHE on-chain (Liquid Threshold)	Live	Threshold VM deployed on GKE
DEX matching engine	Live	1M ops/sec Go, 434M ops/sec GPU
Cross-chain bridge	Live	15+ chains, MPC-backed
Identity (IAM + WebAuthn)	Live	OIDC + WebAuthn, multi-domain
USDL stablecoin	Live	Deployed on mainnet, testnet, devnet
SecurityToken (12,569 assets)	Live	All US equities, ETFs, crypto, bonds on mainnet
LiquidToken (IBITL, BTCL, ETHL)	Live	Liquid Protocol tokens on mainnet
Liquid DEX (21 trading pairs)	Live	IBIT/USDL + 20 pairs, native precompile
Explorer	Live	explore.{main,test,dev}.satschel.com
Options contracts	Ready	OptionsRouter + AmericanOptions in standard lib
Perpetual contracts	Ready	In standard library, pending DEX integration

15 Liquid Protocol: DeFi Composability for Regulated Securities

The core innovation: separate **custody + compliance** (regulated, KYC-gated) from **holding + trading** (permissionless ERC-20).

15.1 Architecture

```
BlackRock IBIT shares
    |
    v
Liquidity ATS (custody + compliance + KYC)
    |
    v
Mint IBITL (IBIT + L suffix) via LiquidToken contract (MPC-controlled)
    |
    +---> Liquid DEX (native precompile, on-chain CLOB)
    +---> Liquid Protocol LPs (permissionless liquidity pool)
    +---> Lending protocols (collateral)
    +---> Options / Perpetuals (on-chain derivatives)
    +---> Direct peer-to-peer transfer (ERC-20)
    |
    v
```

```
Redemption? -> Back through Liquidity ATS (KYC gate)
No redemption needed? -> Hold IBITL, it tracks IBIT 1:1
```

15.2 How It Works

1. **Deposit**: Accredited investor deposits IBIT shares at Liquidity ATS. ATS verifies KYC/AML, confirms share ownership via Alpaca/IBKR.
2. **Mint**: ATS calls `LiquidToken.mint()` on Liquid EVM via 2-of-3 MPC threshold signature (CGGMP21). The underlying IBIT shares are held in custody (Alpaca/BitGo). IBITL is minted 1:1.
3. **Trade**: IBITL is a standard ERC-20 on the Liquid EVM. It can be:
   - Traded on the Liquid DEX (native CLOB precompile, sub-second settlement)
   - Used in Liquid Protocol liquidity pools (IBITL/USDL pair)
   - Deposited as collateral for options and perpetual contracts
   - Used in yield strategies and structured products
   - Transferred peer-to-peer with zero friction
4. **Hold**: Normal users just hold the token. No KYC needed to hold or transfer. The token tracks the underlying 1:1 via NAV oracle.
5. **Redeem**: To convert back to real IBIT shares, go through Liquidity ATS (KYC required). ATS burns IBITL, releases shares.

15.3 Compliance Model

Action	KYC Required?	Why
Mint (deposit shares)	Yes	SEC Reg ATS, accredited investor
Transfer IBITL	No	Standard ERC-20 transfer
Trade on DEX	No	Permissionless liquidity pool
Use as collateral	No	Standard DeFi composability
Redeem (withdraw shares)	Yes	ATS custody gate

Key insight: The compliance boundary is at *mint and redeem*, not at every transfer. This is the same model as USDC (Circle gates mint/redeem, but the token circulates freely) applied to securities.

15.4 Why This Works Legally

1. IBITL is a *Liquid Protocol token*, not a security itself. It represents a 1:1 claim on IBIT shares held in custody at a registered ATS, minted via the `LiquidToken` contract with MPC-controlled mint/burn.
2. The ATS maintains full KYC/AML on all mint and redeem operations.
3. Transfer restrictions (Rule 144, lockup) are enforced at the smart contract level via ERC-1404 hooks on the underlying SecurityToken.
4. The IBITL token inherits compliance from the underlying SecurityToken—if the underlying is restricted (ERC-1404), IBITL cannot be minted.
5. FINRA surveillance monitors all on-chain activity for wash trading, structuring, and market manipulation.

15.5 Dividends, Corporate Actions, and Voting

Securities rights flow only to KYC-verified holders:

Action	Who Receives	Mechanism
Dividends	KYC-verified holders only	TA distributes to whitelisted addresses
Stock splits	All IBITL holders	Contract rebase (automatic, 1:1)
NAV updates	All IBITL holders	Oracle price feed (LiquidFeed precompile)
Voting rights	KYC-verified holders only	On-chain governance (TA-gated)
Tax reporting	KYC-verified holders only	TA generates 1099-DIV, 1099-B
Tender offers	KYC-verified holders only	ATS routes through BD

Key distinction: The token itself is freely transferable (ERC-20). But *regulated rights* (dividends, voting, tax reporting) are only delivered to addresses on the Transfer Agent's whitelist. An anonymous holder gets price exposure. A KYC'd holder gets full securities rights.

This creates a natural incentive to KYC: you can hold IBITL without it, but you miss dividends and cannot redeem. The compliance layer is opt-in at the holder level, mandatory at the mint/redeem level.

15.6 Global Access

Once minted, IBITL is available to the entire Liquid Protocol ecosystem:

- A retail investor in Lagos can hold IBITL without a US brokerage account
- A fund in Singapore can use IBITL as collateral without DTCC membership
- A protocol in Berlin can build yield strategies on IBITL without ATS registration
- Anyone with a Liquid EVM wallet can receive and trade IBITL
- IBITL/USDL trades execute on the native DEX precompile with sub-second finality

The ATS handles the regulated part. The Liquid Protocol handles the rest. Zero friction.

16 Conclusion

The Liquid EVM is not a proposal—it is running infrastructure. The chain is live with post-quantum precompiles. The ATS is matching orders. The MPC cluster is signing transactions. The bridge is moving assets across 15 chains.

17 Latency Arbitrage: Formal Geographic Moat

17.1 Why Kansas City

Equinix KC1 is equidistant from NYSE (New York) and CME (Chicago). Let $d(A, B)$ denote one-way fiber latency between cities A and B.

Theorem 17.1 (Latency Dominance)**.** *For any market participant P colocated at KC1, and any two US exchanges E_1 (NYC), E_2 (Chicago), the maximum latency* $\max(d(P, E_1), d(P, E_2))$ *is minimized at KC1 among all US cities.*

Proof sketch. NYC $\leftrightarrow$ Chicago fiber: $\sim$12.98ms. KC sits at the geographic midpoint: $d(\text{KC}, \text{NYC}) \approx 8\text{ms}$, $d(\text{KC}, \text{CHI}) \approx 4\text{ms}$, so max = 8ms. Any city closer to one exchange is farther from the other. By the triangle inequality, KC minimizes the maximum. $\square$

17.2 International Latency Table

The following table presents measured one-way fiber latencies from the KC1 colocation facility to major global financial centers. All values reflect production-grade dark fiber or lit wavelength paths; satellite and microwave alternatives are excluded.

City	Exchange/Role	One-Way (ms)	Round-Trip (ms)
Kansas City	Liquid EVM (colocated)	0	<1
St. Louis	Regional connectivity hub	∼2	∼4
Chicago	CME, CBOE	∼4	∼8
New York	NYSE, Nasdaq	∼8	∼16
London	LSE, ICE Futures	∼42	∼84
Frankfurt	Eurex, Deutsche Börse	∼48	∼96
São Paulo	B3 (Bovespa)	∼55	∼110
Mumbai	BSE, NSE India	∼95	∼190
Singapore	SGX	∼100	∼200
Tokyo	JPX (TSE)	∼67	∼134
Shanghai	SSE, SHFE	∼75	∼150
Beijing	CFFEX	∼77	∼154
Pyongyang	—	∼85	∼170

Table 1: One-way fiber latency from Equinix KC1 to global financial centers. Speed of light in fiber ≈ 200,000 km/s. These are physical lower bounds; actual production latencies are 5–15% higher due to routing overhead.

17.3 US Arbitrage Sovereignty

Theorem 17.2 (Trans-Pacific Arbitrage Barrier)**.** *For any non-US market participant A located at distance $d(A, KC1)$ and any US-colocated participant P at KC1, the round-trip latency advantage of P over A satisfies $\Delta = 2 \cdot d(A, KC1) - 2 \cdot d(P, E) \geq 120ms$ for all A outside North America.*

Proof. The minimum trans-Pacific fiber path (Tokyo → Los Angeles → KC1) incurs ∼67ms one-way. US colocation at KC1 reaches NYSE in 8ms and CME in 4ms. Round-trip difference: $2(67) - 2(8) = 118$ms. For Beijing via Tokyo relay, add ∼10ms, giving $\Delta \geq 138$ms. For London (42ms one-way), $\Delta = 2(42) - 2(8) = 68$ms. For any Asian city, $\Delta \geq 118$ms. □

This is not a software optimization. It is a consequence of the speed of light in optical fiber (≈ 200,000 km/s) and the geographic position of the continental United States. No algorithm, no hardware upgrade, and no protocol change can overcome it. The latency advantage is permanent, unforkable, and enforced by physics.

Theorem 17.3 (US Arbitrage Sovereignty)**.** *Let S be any security traded on the Liquid EVM with matching engine colocated at KC1. For any foreign entity F located at distance $d_F > 500km$ from KC1, and any US-colocated entity U at KC1, U observes and responds to price changes on S before F can submit an arbitrage order. No foreign entity can extract latency arbitrage value from US-settled securities.*

Proof. At 500km, one-way fiber latency is ≥2.5ms. The ZAP protocol round-trip from KC1 is 42μs. Any entity at $d > 500$km incurs round-trip overhead of ≥5ms, giving the colocated participant a $5\text{ms} - 0.042\text{ms} = 4.958$ms head start. At the Liquid DEX matching rate of 1M orders/sec, 4.958ms accommodates 4,958 order operations. No foreign latency arbitrageur can profitably front-run a colocated US participant. □

Corollary 17.4 (Break-Even Distance)**.** *The break-even distance at which a remote participant loses its latency advantage over KC1 colocation is approximately 500km (one-way fiber: 2.5ms, round-trip: 5ms). Beyond this radius, the colocated participant wins every latency race. St. Louis (2ms), Chicago (4ms), and Kansas City metro are within the competitive zone. No international city is.*

17.4 Settlement Capital Efficiency: $105B/yr Opportunity

T+1 settlement on NYSE/Nasdaq traps capital overnight. For every trade executed today, the buyer's cash and the seller's shares are locked for 24 hours until settlement. This creates an enormous opportunity cost.

Theorem 17.5 (T+1 Overnight Capital Lockup)**.** *Let V denote total daily US equity settlement volume. The annual opportunity cost of T+1 settlement at risk-free rate r is:*

$$C_{T+1} = V \times \frac{r}{252}$$

where 252 is the number of trading days per year.

For 2025 US equity markets: daily settlement volume $V \approx \$2.1$ trillion (DTCC average). At the current risk-free rate $r = 5.0\%$ (Fed Funds effective rate, Q1 2026):

$$C_{\text{T+1}} = \$2.1\text{T} \times \frac{0.05}{252} = \$416.7\text{M per trading day}$$

$$C_{\text{annual}} = \$416.7\text{M} \times 252 = \boxed{\$105.0\text{B/yr}}$$

This $105 billion per year is pure deadweight loss—capital that earns zero return while locked in settlement. On the Liquid EVM, settlement is T+0 (sub-second). Every dollar of settlement float is freed immediately for reinvestment, lending, or redeployment.

For BlackRock specifically, with $11.5T AUM and average portfolio turnover of 25% annually, the capital freed by T+0 settlement is:

$$\text{BlackRock T+0 benefit} = \$11.5\text{T} \times 0.25 \times \frac{0.05}{252} \approx \$5.7\text{M/day} = \$1.44\text{B/yr}$$

17.5 Settlement Revenue Repatriation: $3.65B/yr

DTCC (Depository Trust & Clearing Corporation) [44] charges approximately $0.005 per settled transaction. With approximately 2 billion equity transactions settled annually in the US:

$$\text{DTCC settlement revenue} \approx 2\text{B} \times \$0.005 = \$10\text{B/yr (estimated)}$$

More conservatively, DTCC's disclosed revenue from clearing and settlement services is approximately $2–4B/yr. On the Liquid EVM, settlement is native—there is no clearinghouse intermediary. The ATS, BD, and TA operate under one regulatory umbrella. The settlement fee structure:

- **On-chain gas**: <$0.001 per settlement (Liquid EVM block space)
- **ATS fee**: 0–25bp (volume tiered, see fee schedule)
- **DTCC fee**: $0 (eliminated entirely)

At an estimated $3.65B/yr in DTCC settlement fees attributable to ETF products (approximately 35% of total, given ETF trading volume share), moving ETF settlement to the Liquid EVM repatriates this revenue to the exchange operator and its participants.

17.6 On-Chain vs Traditional Latency

18 Market Making and Revenue Model

18.1 Fee Structure

18.2 Revenue Projections

If BlackRock's IBIT ($50B AUM) achieves 2% daily turnover on-chain:

Operation	Liquid EVM	NYSE	Speedup
Order submission	42μs (ZAP)	100μs	2.4×
Matching	<1μs	∼10μs	10×
Settlement	<500ms	86,400,000ms (T+1)	172,800×
Finality	<500ms	86,400,000ms	172,800×
Cross-listing new asset	Minutes	Months	>10,000×
Capital lockup	0	24 hours	∞
Settlement fee	<$0.001	$0.005+ (DTCC)	5×+

Tier	30-Day Volume	Taker / Maker
Retail	<$1M	25bp / 10bp
Institutional	$1M–$100M	15bp / 5bp
Market Maker	>$100M	10bp / 0bp (rebate)
BlackRock (custom)	Negotiated	Flat fee per ETF

- Daily volume: $1B
- At 15bp taker fee: $1.5M/day revenue
- Annual: $547M (vs. NYSE listing fees of ∼$200K/year)

The 10,000× premium over NYSE listing reflects the value of instant settlement, 24/7 trading, fractional shares, and global access.

18.3 Impermanent Loss Protection

For liquidity pools, the Liquid DEX LiquidPool precompile implements concentrated liquidity with automatic rebalancing. Market makers providing liquidity for IBIT/USDL pools receive:

- Trading fee share (pro-rata to liquidity)
- LQDTY staking rewards
- IL protection via the protocol insurance fund (funded by 5% of fees)

19 LQDTY Token Economics

Property	Value
Token	LQDTY (ERC-20 on Liquid EVM)
Supply	10,000,000,000 (10B)
Decimals	18
Chain ID	8675309 (mainnet)
Dollar token	USDL (1:1 USD, ACH-backed)

19.1 Fee Burn Mechanism

5% of all trading fees are used to buy and burn LQDTY, creating deflationary pressure proportional to exchange volume. At $1B daily volume, this removes ∼$75K/day in LQDTY from circulation.

19.2 Governance

LQDTY holders vote on:

- Fee tier adjustments

- New asset listings (SecurityToken whitelist)
- Protocol upgrades (Liquid EVM hard forks)
- Insurance fund allocation
- Validator set changes

20 Formal Verification

All critical components have machine-checked proofs (Lean 4):

Component	Property	Proof
Quasar consensus	Height monotonicity, BLS quorum	[17]
CGGMP21 signing	Threshold ECDSA composition	[20]
FROST signing	Schnorr threshold axioms	[19]
LSS reshare	Secret sharing correctness	[21]
Ringtail PQ	Lattice threshold axioms	[18]
TFHE gates	Bootstrap correctness	[22]
ML-DSA	Module lattice signature	[23]
Teleport bridge	E2E deposit-yield-teleport safety	[24]

20.1 Exchange Correctness

The matching engine satisfies:

Theorem 20.1 (Price-Time Priority)**.** *For any two orders o_1, o_2 with $price(o_1) = price(o_2)$ and $time(o_1) < time(o_2)$, the engine matches o_1 before o_2.*

Theorem 20.2 (Atomic Settlement)**.** *For any matched trade (o_{buy}, o_{sell}), either both the SecurityToken transfer and USDL transfer execute, or neither does. No partial settlement state is observable.*

Theorem 20.3 (Compliance Preservation)**.** *For any transfer τ of SecurityToken S from address a to b, τ succeeds if and only if $whitelist(S, b) \wedge accredited(b) \wedge \neg locked(S, a)$.*

21 BlackRock-Specific Value Propositions

The following capabilities are designed for the specific operational requirements of BlackRock and institutional asset managers of comparable scale. Each integrates directly with the Liquid EVM infrastructure described in preceding sections.

21.1 Portfolio Rebalancing via FHE

BlackRock rebalances approximately $100B across 1,000+ ETFs on a quarterly basis. On traditional rails, rebalancing telegraphs intent: the moment BlackRock's orders hit the market, front-runners extract value.

On the Liquid EVM, the entire rebalancing workflow executes on encrypted state. The portfolio optimizer receives encrypted current holdings, encrypted target weights, and encrypted market prices. It produces encrypted trade instructions that the ATS executes against the encrypted dark pool.

Listing 8: Encrypted portfolio rebalancing across 1000 ETFs

```
// RebalanceEncrypted computes trade instructions from encrypted
// current holdings and encrypted target weights.
```

```
func RebalanceEncrypted(
    current []*EncryptedPosition, // 1000+ encrypted positions
    targets []*EncryptedWeight,   // encrypted target allocations
    navCT   *tfhe.Ciphertext,     // encrypted total NAV
    eval    *tfhe.Evaluator,
) []*EncryptedTrade {
    trades := make([]*EncryptedTrade, len(current))
    for i, pos := range current {
        // target value = NAV * target weight
        targetVal := eval.Mul(navCT, targets[i].WeightCT)
        // current value = quantity * price
        currentVal := eval.Mul(pos.QtyCT, pos.PriceCT)
        // delta = target - current (encrypted)
        delta := eval.Sub(targetVal, currentVal)
        // trade quantity = delta / price
        tradeQty := eval.Div(delta, pos.PriceCT)
        trades[i] = &EncryptedTrade{
            AssetID: pos.AssetID,
            QtyCT:   tradeQty,
        }
    }
    return trades // execute against encrypted dark pool
}
```

At no point does any market participant, exchange operator, or network validator observe the rebalancing trades. The estimated value leakage prevented: 5–15bp per rebalancing event $\times$ \$100B = \$50–150M per quarterly rebalance.

21.2 Social/Copy Trading with Encrypted Leader Portfolios

The platform supports copy trading where retail investors replicate the positions of professional portfolio managers. The leader's portfolio is encrypted; followers copy trades without observing the leader's holdings.

The mechanism: the leader's portfolio state is an FHE ciphertext. When the leader rebalances, the encrypted trade instructions are replicated to each follower's encrypted portfolio, scaled by the follower's account size. The follower sees only their own positions (decrypted with their passkey). The leader's alpha—the specific weights and timing—remains confidential.

This creates a new revenue stream: subscription fees for copy trading access, with cryptographic guarantee that the leader's strategy cannot be reverse-engineered.

21.3 24/7 ETF Secondary Market

Traditional ETF trading is limited to 6.5 hours per day (9:30 AM – 4:00 PM ET), 5 days per week. On the Liquid EVM, SecurityToken ETFs trade 24/7/365 with:

- **Fractional shares**: Buy \$1 of IBIT (minimum on NYSE: 1 share $\approx$ \$50)
- **Global access**: Any KYC-verified investor worldwide, any timezone
- **Instant settlement**: T+0, not T+1 (US) or T+2 (international)
- **No market hours**: Asia, Europe, Americas trade the same IBIT simultaneously
- **Atomic cross-asset**: Swap IBIT for AGG in a single atomic transaction

The revenue opportunity from after-hours ETF trading: US ETFs saw \$3.2T in daily volume in 2025. Extending trading hours from 6.5 to 24 hours represents a 3.7$\times$ increase in available trading time. Even capturing 10% of the proportional volume increase yields \$1.2T in incremental annual volume.

21.4 BUIDL Integration and Bridge

BlackRock's BUIDL ($1.7B tokenized treasury fund, Ethereum ERC-20) bridges to the Liquid EVM via the MPC-backed cross-chain bridge [13]. On the Liquid EVM, BUIDL can serve as:

- **Margin collateral**: Post BUIDL as margin for ETF trading (yield-bearing collateral, superior to USDC)
- **Fee subsidy**: BUIDL yield offsets trading fees for large accounts
- **Native reissuance**: Reissue BUIDL natively on Liquid EVM with FHE-encrypted holdings, Quasar finality, and SecurityToken compliance hooks
- **Cross-collateral**: Use BUIDL yield to fund IBIT pool liquidity

The bridge uses CGGMP21 threshold MPC (2-of-3 shards: BlackRock, Liquidity, independent custodian) for lock-and-mint operations. Bridge latency: <30s including Ethereum finality confirmation.

21.5 Authorized Participant Creation/Redemption

AP creation and redemption (the mechanism that keeps ETF prices aligned with NAV) runs as an encrypted sealed-bid auction (Section 4.4). This eliminates the current information asymmetry where APs can observe each other's creation/redemption activity and extract arbitrage.

The creation unit size (currently 25,000–100,000 shares for most BlackRock ETFs) can be reduced to arbitrary minimums on-chain, enabling smaller APs to participate and increasing competition. More competition in the AP market reduces tracking error and tightens bid-ask spreads for end investors.

21.6 Tax-Loss Harvesting on Encrypted Cost Basis

FHE enables automated tax-loss harvesting without revealing the investor's cost basis, gain/loss positions, or tax strategy:

Listing 9: Tax-loss harvesting on encrypted cost basis

```
// HarvestLosses identifies positions with unrealized losses
// and generates sell instructions, all on encrypted data.
func HarvestLosses(
    positions []*EncryptedTaxLot,
    eval      *tfhe.Evaluator,
) []*EncryptedTrade {
    var trades []*EncryptedTrade
    for _, lot := range positions {
        // unrealized P&L = current value - cost basis (encrypted)
        currentVal := eval.Mul(lot.QtyCT, lot.CurrentPriceCT)
        pnl := eval.Sub(currentVal, lot.CostBasisCT)
        // isLoss = (pnl < 0) -- encrypted boolean
        isLoss := eval.LT(pnl, eval.EncryptUint64(0))
        // Generate sell trade only for losses (encrypted conditional)
        sellQty := eval.Mux(isLoss, lot.QtyCT, eval.EncryptUint64(0))
        if true { // always append; zero-qty trades are no-ops
            trades = append(trades, &EncryptedTrade{
                AssetID: lot.AssetID,
                QtyCT:   sellQty,
            })
        }
    }
    return trades
}

type EncryptedTaxLot struct {
```

```
    AssetID        string
    QtyCT          *tfhe.Ciphertext // encrypted quantity
    CostBasisCT    *tfhe.Ciphertext // encrypted total cost basis
    CurrentPriceCT *tfhe.Ciphertext // encrypted current market price
    AcquiredDateCT *tfhe.Ciphertext // encrypted acquisition timestamp
}
```

The investor's tax situation is never exposed to the exchange, the ATS, or any counterparty. The tax engine produces encrypted sell orders that the ATS executes against the encrypted dark pool. IRS reporting uses threshold decryption with the investor's tax advisor as a required committee member.

21.7 Real-Time Risk Management on Encrypted Positions

Risk management across all BlackRock funds operates on encrypted position data. Value-at-Risk (VaR), stress testing, and scenario analysis run as FHE circuits:

Listing 10: Encrypted VaR computation across all funds

```
// ComputeEncryptedVaR calculates portfolio Value-at-Risk
// on encrypted positions across all funds.
func ComputeEncryptedVaR(
    funds      []*EncryptedFund,
    confidence float64, // e.g., 0.99 for 99% VaR
    eval       *tfhe.Evaluator,
) *tfhe.Ciphertext {
    // Aggregate encrypted exposure across all funds
    totalExposure := eval.EncryptUint64(0)
    for _, fund := range funds {
        for _, pos := range fund.Positions {
            posVal := eval.Mul(pos.QtyCT, pos.PriceCT)
            totalExposure = eval.Add(totalExposure, posVal)
        }
    }
    // VaR = totalExposure * volatility * z-score (encrypted arithmetic)
    zScore := eval.EncryptUint64(uint64(confidence * 1000))
    volCT := eval.EncryptUint64(20) // 20% annualized vol (encrypted)
    dailyVol := eval.Div(volCT, eval.EncryptUint64(16)) // sqrt(252) ~ 16
    varCT := eval.Div(eval.Mul(eval.Mul(totalExposure, dailyVol), zScore)
        ,
        eval.EncryptUint64(1000))
    return varCT
}
```

The risk management system produces encrypted risk metrics. The CRO receives threshold-decrypted aggregates (total VaR, sector concentration, liquidity coverage ratio). Individual fund positions remain encrypted. Cross-fund exposure analysis—critical for systemic risk assessment—runs without any single person observing the positions of all funds simultaneously.

22 Why BlackRock Deploys on Liquid EVM

The case reduces to eight facts:

1. **Legal authority**: Only platform with ATS + BD + TA + L1 + DEX + PQ. tZero has ATS but no chain. Ethereum has a chain but no ATS.

2. **Instant settlement**: T+0 vs T+1 eliminates $105B/yr in industry-wide overnight capital lockup costs. For BlackRock alone: $1.44B/yr freed.

3. **Quantum safety**: FIPS 203/204/205 precompiles active at genesis. 30-year fiduciary obligation demands PQ security today.

4. **Confidential compliance**: FHE enables encrypted dark pools, private rebalancing, confidential NAV, and zero-knowledge compliance proofs with regulatory threshold decryption. No other chain has this.

5. **Geographic moat**: KC colocation gives 120ms+ structural advantage over non-US participants. Break-even at 500km. Physical law, not software.

6. **Non-custodial**: 2-of-3 MPC where BlackRock holds their own shard. They can exit independently. Zero counterparty risk.

7. **Revenue repatriation**: $3.65B/yr in DTCC settlement fees for ETF products is eliminated by on-chain settlement.

8. **24/7 global market**: Extends ETF trading from 6.5 hours/day to 24/7 with fractional shares, instant settlement, and global access.

The regulatory moat is the key differentiator. Any blockchain can add an orderbook. No blockchain has SEC-registered ATS + BD + TA licenses. That combination took years of regulatory work and cannot be replicated quickly.

For an institution managing $11.5 trillion, the question is not whether securities will move on-chain—it is which chain has the legal authority to settle them. Liquidity.io is that chain.

This document describes deployed infrastructure verified against source code as of April 2026. All performance figures are from benchmarks on the cited hardware. Regulatory status refers to Satschel, Inc. registrations.

References

[1] Kelling, Z. and Bin, W. *Lux Consensus: Physics-Inspired Metastable Blockchain Consensus*. Lux Partners Limited, 2020. https://github.com/luxfi/papers/raw/main/pdfs/lux-consensus.pdf

[2] Kelling, Z. and Bin, W. *Quantum Consensus: Post-Quantum Cryptography with ML-DSA Signatures*. Lux Industries, 2024. https://github.com/luxfi/papers/raw/main/pdfs/lux-quantum-consensus.pdf

[3] Kelling, Z. and Bin, W. *FPC: Fast Probabilistic Consensus with Adaptive Thresholds*. Lux Industries, 2024. https://github.com/luxfi/papers/raw/main/pdfs/lux-fpc-consensus.pdf

[4] Kelling, Z., Seesahai, V., and Bin, W. *Quasar Consensus: Dual-Certificate Quantum-Secure Finality (BLS + Ringtail)*. Lux Industries, 2024. (Post-FPC; builds on Ringtail lattice threshold signatures.) https://github.com/luxfi/papers/raw/main/pdfs/lux-quasar-consensus.pdf

[5] Kelling, Z. and Worring, A. *NTT Transform: 85% Gas Reduction for Post-Quantum Crypto on EVM*. Lux Partners Limited, 2021. https://github.com/luxfi/papers/raw/main/pdfs/lux-ntt-transform.pdf

[6] Kelling, Z. and Seesahai, V. *Universal Threshold Signatures: Unified Framework (CMP, FROST, LSS, Doerner, Ringtail)*. Lux Partners Limited, 2021. https://github.com/luxfi/papers/raw/main/pdfs/lux-universal-threshold-signatures.pdf

[7] Kelling, Z. and Worring, A. *FHE coprocessor: Privacy-Preserving Smart Contracts (zkEVM, FHE, TEE)*. Lux Partners Limited, 2021. https://github.com/luxfi/papers/raw/main/pdfs/lux-zchain.pdf

[8] Kelling, Z., Bin, W., and Seesahai, V. *Liquid Threshold: MPC Threshold Custody (CGGMP21, MuSig2, FROST, Ringtail)*. Lux Partners Limited, 2023. https://github.com/luxfi/papers/raw/main/pdfs/lux-mchain-mpc.pdf

[9] Kelling, Z. and Worring, A. *EVM Precompiles: Post-Quantum Cryptographic Primitives for Blockchain*. Lux Industries, 2024. https://github.com/luxfi/papers/raw/main/pdfs/lux-evm-precompiles.pdf

[10] Kelling, Z. and Seesahai, V. *Ringtail: Lattice-Based Threshold Signatures for Post-Quantum MPC*. Lux Partners Limited, 2020. (Initial lattice threshold construction; refined 2024–2025 for Quasar integration.) https://github.com/luxfi/papers/raw/main/pdfs/lux-ringtail-pq.pdf

[11] Kelling, Z. and Seesahai, V. *Lightspeed DEX: HFT-Optimized Decentralized Exchange*. Lux Partners Limited, 2019. https://github.com/luxfi/papers/raw/main/pdfs/lux-lightspeed-dex.pdf

[12] Kelling, Z., Bin, W., and Seesahai, V. *Teleport Protocol: Trustless Cross-Chain Asset Transfer via Light Client Verification*. Lux Partners Limited, 2022. https://github.com/luxfi/papers/raw/main/pdfs/lux-teleport-protocol.pdf

[13] Kelling, Z., Bin, W., and Seesahai, V. *Lux Bridge: Cross-Chain with ZK Light Clients and IBC Integration*. Lux Partners Limited, 2023. https://github.com/luxfi/papers/raw/main/pdfs/lux-bridge.pdf

[14] Kelling, Z. and Bin, W. *Verkle Trees: Constant-Size Proofs (∼150 bytes) for Stateless Clients*. Lux Partners Limited, 2022. https://github.com/luxfi/papers/raw/main/pdfs/lux-verkle-trees.pdf

[15] Kelling, Z. and Worring, A. *TEE Computing Mesh: Distributed TEE Network for Confidential Computing*. Lux Industries, 2024. https://github.com/luxfi/papers/raw/main/pdfs/lux-tee-computing-mesh.pdf

[16] Kelling, Z. and Seesahai, V. *Warp Messaging: Cross-Subnet Communication Protocol*. Lux Partners Limited, 2023. https://github.com/luxfi/papers/raw/main/pdfs/lux-warp-messaging.pdf

[17] Kelling, Z. and Bin, W. *Formal Proof: Quasar Protocol — Height Monotonicity and BLS Quorum*. Lean 4. Lux Industries, 2024. https://proofs.lux.network

[18] Kelling, Z. and Seesahai, V. *Formal Proof: Ringtail — Lattice-Based Threshold Signature Axioms*. Lean 4. Lux Industries, 2024–2025. (Covers both the 2020 construction and 2024 Quasar-integrated variant.) `https://proofs.lux.network`

[19] Kelling, Z. and Seesahai, V. *Formal Proof: FROST Threshold — Schnorr Threshold Signature Axioms*. Lean 4. Lux Partners Limited, 2021. `https://proofs.lux.network`

[20] Kelling, Z., Bin, W., and Seesahai, V. *Formal Proof: CGGMP21 — Threshold ECDSA Composition*. Lean 4. Lux Partners Limited, 2023. `https://proofs.lux.network`

[21] Kelling, Z. and Seesahai, V. *Formal Proof: LSS — Linear Secret Sharing Reshare Correctness*. Lean 4. Lux Partners Limited, 2021. `https://proofs.lux.network`

[22] Kelling, Z. and Worring, A. *Formal Proof: TFHE — Torus FHE Gate Bootstrapping Correctness*. Lean 4. Lux Industries, 2025. `https://proofs.lux.network`

[23] Kelling, Z. *Formal Proof: ML-DSA — Module Lattice Digital Signature Axioms*. Lean 4. Lux Industries, 2024. `https://proofs.lux.network`

[24] Kelling, Z., Bin, W., and Seesahai, V. *Formal Proof: E2E Teleport Safety — Bridge-Deposit-Yield-Teleport Pipeline*. Lean 4. Lux Partners Limited, 2022. `https://proofs.lux.network`

[25] Kelling, Z. *Custody Architecture Audit: From Custodial SSS to Non-Custodial MPC*. Satschel, Inc., April 2026.

[26] Canetti, R., Gennaro, R., Goldfeder, S., Makriyannis, N., and Peled, U. *UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts*. ACM CCS, 2020. `https://eprint.iacr.org/2021/060`

[27] Komlo, C. and Goldberg, I. *FROST: Flexible Round-Optimized Schnorr Threshold Signatures*. SAC 2020, LNCS 12804, pp. 34–65, 2021.

[28] Chillotti, I., Gama, N., Georgieva, M., and Izabachène, M. *TFHE: Fast Fully Homomorphic Encryption over the Torus*. Journal of Cryptology, 33(1):34–91, 2020. `https://eprint.iacr.org/2018/421`

[29] Music, J., Huber, R., and Kegelmann, A. *ERC-3643: T-REX — Token for Regulated Exchanges*. Ethereum Improvement Proposals, EIP-3643, 2021.

[30] Daian, P. et al. *Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability*. IEEE S&P, pp. 910–927, 2020.

[31] National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203, August 2024. `https://csrc.nist.gov/pubs/fips/203/final`

[32] National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*. FIPS 204, August 2024. `https://csrc.nist.gov/pubs/fips/204/final`

[33] National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*. FIPS 205, August 2024. `https://csrc.nist.gov/pubs/fips/205/final`

[34] Securities and Exchange Commission. *Regulation of Exchanges and Alternative Trading Systems*. SEC Release No. 34-40760, 17 CFR Parts 202, 240, 242, 249, 1998.

[35] Securities and Exchange Commission. *Persons Deemed Not to Be Engaged in a Distribution*. 17 CFR §230.144, 1972 (as amended).

[36] Securities and Exchange Commission. *Regulation D: Limited Offer and Sale of Securities Without Registration*. 17 CFR §§230.501–508, 1982 (as amended).

[37] BlackRock, Inc. *2024 Annual Report and Form 10-K*. SEC EDGAR, February 2025.

[38] National Institute of Standards and Technology. *Security Requirements for Cryptographic Modules*. FIPS 140-3, March 2019. `https://csrc.nist.gov/pubs/fips/140-3/final`

[39] Securities and Exchange Commission. *Investment Company Names (the "Names Rule")*. SEC Rule 35d-1, 17 CFR §270.35d-1, 2001 (amended November 2023).

[40] Securities and Exchange Commission. *Investment Company Act of 1940*. 15 U.S.C. §§80a-1 et seq., 1940 (as amended).

[41] Securities and Exchange Commission. *Regulation NMS: National Market System*. SEC Release No. 34-51808, 17 CFR Parts 200, 201, 230, 240, 242, 249, 270, 2005.

[42] Financial Industry Regulatory Authority. *FINRA Rule 5310: Best Execution and Interpositioning*. FINRA Manual, 2014 (as amended).

[43] Securities and Exchange Commission. *Shortening the Securities Transaction Settlement Cycle*. SEC Release No. 34-96930, 17 CFR Parts 232 and 240, February 2023. (Effective T+1: May 28, 2024.)

[44] Depository Trust & Clearing Corporation. *DTCC 2024 Annual Report: Settlement and Clearing Statistics*. DTCC, March 2025.

[45] BlackRock, Inc. and Securitize Markets, LLC. *BlackRock USD Institutional Digital Liquidity Fund (BUIDL)*. Launched March 2024 on Ethereum. $1.7B AUM as of Q1 2026.

[46] Kelling, Z. and Seesahai, V. *Liquid EVM: A Sovereign Post-Quantum Blockchain for Regulated Securities*. Satschel, Inc., April 2026.

[47] Kelling, Z., Bin, W., and Seesahai, V. *Formal Proof: Cross-Chain Bridge — Lock-Mint-Burn Safety*. Lean 4. Lux Partners Limited, 2023. `https://proofs.lux.network`