Open Captable Protocol (OCP): An Interopable Solution for Securities Settlement and Captable Management Onchain

Victor Mimo

January 30, 2025

Abstract

The Open Captable Protocol (OCP) introduces a revolutionary approach to managing capitalization tables through blockchain technology. This paper presents a comprehensive solution that bridges the gap between traditional security transfer systems and modern blockchain capabilities, while maintaining compliance and data privacy standards.

1 Introduction

1.1 The Gap Between Web3 & Securities Settlement

- Securities settlement remains primarily off-chain and fragmented, limiting interoperability.
- This is a problem because Web3 thrives on interoperability and permissionless (or sufficiently permissionless) actions.
- Wallets, DeFi, and protocols interoperate, yet captables remain siloed in Web2.
- Every crypto company today still uses Web2 databases to track cap tables.
- Even Coinbase explored going public on-chain but was laughed at (Coin documentary).
  - This wasn't about captables—it was about the missing financial infrastructure (investment banks, liquidity, etc.).
- On-chain captables seem unrealistic today—but why?
  - Is it cost? Regulation? Lack of a standard?
- Blockchains enable clearing, but settlement is still undefined.
- There is no standard on-chain framework for tracking securities ownership.
- Some have proposed hybrid approaches—such as Balaji's "Mirrortables" (2021), which mirrored Web2 cap tables on-chain.
  - But mirroring isn't enough—it still treats legacy systems as primary.
  - OCP flips this model: on-chain becomes the source of truth, and legacy systems can export into OCP—but OCP does not rely on them.
- The missing piece isn't just technical—it's about adoption.
  - To bring securities fully on-chain, we need to invest in this infrastructure today.
- *[Note: Settlement layers today: Tokenized securities exist on Base, Polygon, Solana, Ethereum—what's the right layer?]*

1.2 What OCP Solves

- Built on Open Captable Format (OCF), a trusted and widely adopted standard in Web2.
- A fully on-chain, event-driven captable that is immutable, auditable, efficient, and scalable.
- Future-proofed to support more asset types as tokenized finance expands.
- Interoperable securities that protocols can integrate with natively for seamless ownership tracking and trading.
- Already in production, tracking over $1B in private assets.

2 Event-Based Smart Contract Captable

2.1 Common Misconceptions and Reality

- Captables are widely seen as a boring back-office necessity—whether they live in Excel, a database, or a SaaS platform, they "just exist" and don't add value.
- Many assume putting captables on-chain is unnecessary—they see it as over-engineering something that doesn't need innovation.
- People think captables "get in the way" of trading—a compliance burden that doesn't contribute to market efficiency.
- But an on-chain captable isn't just a better record-keeping tool—it creates a network of interoperable securities.
- Read & write permissions are granted/removed with code, making securities management programmable and composable.
- This isn't just about tracking ownership—it's about making ownership actionable across protocols.
- People once thought fiat currency didn't need to be on-chain—but stablecoins changed that. OCP does the same for securities.

3 OCP's Breakthrough

- **OCP is Fully Native & Modular (Cross-Chain Compatible)**
  - Unlike hybrid models that mirror Web2, OCP is fully native—legacy systems can export into OCP, but OCP does not rely on them.
  - OCP's architecture is modular, meaning the core framework works across blockchains.
- **Event-Driven Captables as the Core Model**
  - Captables derive state from event-driven transactions, rather than mutable records.
  - ActivePositions tracks ownership without external oracles or unnecessary disclosure.
  - New facets (EVM) or programs (Solana) can be added dynamically to support evolving financial models.
- **Blockchain-Specific Implementations**

- On EVM, we use the Diamond Architecture to enable scalable, gas-efficient captable growth.
- On Solana & other chains, different scaling methods will be used, but the core OCP model remains the same.
- This ensures OCP is future-proof, allowing it to evolve as blockchain architectures improve.

4 Why This Is a Fundamental Shift

- **Securities as Interoperable Financial Primitives**
  - In Web2, captables are static records that sit in private databases.
  - In OCP, ownership can be used in smart contracts, DeFi, DAOs, and programmable markets.
  - Just as stablecoins made fiat programmable, OCP makes securities programmable.
- **From Compliance Burden to Programmable Governance**
  - Traditionally, captables are compliance-first—designed for filings, not flexibility.
  - With OCP, ownership is a live data layer, where permissions, governance, and transfers can be enforced at the smart contract level.
  - This removes operational overhead while maintaining regulatory compliance.
- **A New Layer for Capital Markets**
  - Traditional finance is stuck with slow, fragmented infrastructure.
  - OCP lays the foundation for real-time settlement, multi-chain securities, and global capital formation.
- **No More Vendor Lock-In: Full Ownership Control**
  - In Web2, switching cap table providers (e.g., Carta → Pulley) requires a full export and legal migration.
  - With OCP, switching services doesn't require migration—just an ownership update on an already-deployed captable.
  - Companies stay in control, eliminating data lock-in and making cap tables truly portable.

5 Interoperability

5.1 Two Types of Interoperability

1. Protocol-Level Interoperability:

- OCP isn't just a captable—it's a financial primitive that other protocols can build on.
- Other protocols (e.g., broker-dealers, issuance platforms, automated market makers) can become operators in OCP.
- RBAC (Role-Based Access Control) enables fine-grained permissioning, allowing external protocols to execute actions on behalf of an entity.

  - Example: A solar security issuance protocol can let a trading platform handle secondary transactions without needing a full export of captable data.
  - Example: A DeFi lending protocol can verify holdings in OCP to enable tokenized securities as collateral without requiring manual attestations.

- This removes the bottlenecks of traditional financial reconciliation, where counterparties need manual data access—OCP makes securities live, programmable, and interoperable.

2. Proof-of-Ownership with StakeholderNFT:

- OCP is extensible—protocols can build new layers on top of the captable.
- StakeholderNFT is one example of how ownership can be used beyond record-keeping.
- Investors can mint an NFT that dynamically reflects their holdings—proving ownership without exposing sensitive details.
  - Privacy-Preserving: An investor can prove they hold shares in a company without revealing the exact number or valuation.
  - Useful for governance, token-gated access, and reputation-based systems where full transparency isn't needed.
- This enables governance, token-gated apps, identity verification, and DeFi collateralization.
- **Key Takeaway:** Ownership on OCP isn't just a static database entry—it's composable, verifiable, and programmable.

6 Future Challenges and Long-term Vision

6.1 The Problem: Multi-Chain Market Contracts, Fragmented Settlement

- A solar field protocol deploys market contracts across multiple blockchains to maximize liquidity.
- Each chain records trades, but settlement needs to be unified.
- Right now, options might be:
  - Deploying the captable on each chain (inefficient, complex).
  - Using oracles or bridging solutions (potential trust assumptions).

6.2 The Vision: One Source of Truth for Settlement

- Whether a security is traded on Ethereum, Solana, Base, or another chain, there's one final authoritative record.
- The captable itself isn't fragmented—it syncs updates from multiple chains back to a unified source of truth.

6.3 Three Possible Approaches to Achieving This Vision

6.3.1 1. Circle-Style API Model (Centralized Syncing & On-Chain Settlement)

- A single entity (e.g., OCP Foundation) provides a cross-chain settlement API, similar to Circle's CCTP for USDC.
- Market contracts on multiple chains submit settlement events to a centralized service, which updates the captable.
- Smart contracts call the API to ensure on-chain finality, reducing fragmentation.
- **Challenges:**
  - Requires a Web2 component (API calls).
  - Introduces trust assumptions similar to how USDC relies on Circle.

6.3.2 2. On-Chain Cross-Chain Messaging (LayerZero/IBC-Style)

- Uses cross-chain messaging protocols like LayerZero, Axelar, or IBC to relay settlement updates between chains.
- Ownership is only updated when messages are verified by the captable contract on the primary chain.
- **Challenges:**
  - Cross-chain bridges have security risks.
  - Latency and finality differences between chains could cause syncing delays.
  - Gas costs could be prohibitively high.

6.3.3 3. A Global Settlement Chain (Celestia-Style)

- Instead of choosing a specific blockchain like Ethereum or Solana, OCP could operate on a dedicated "Settlement Layer."
- Every trade on any chain must be reported to this single ledger, which serves as the canonical source of truth.
- Other chains would read from this chain when validating ownership.
- **Challenges:**
  - Requires industry adoption—getting every protocol to agree on a single ledger is difficult.
  - Gas fees—every security transaction needs to be committed to this chain.

6.4 Next Steps & Research Areas

- Initially, OCP may explore the Circle-Style API model, as it is the most feasible short-term solution.
- Over time, cross-chain messaging or a dedicated settlement layer may provide a more trustless and decentralized approach.
- A key research focus is defining finality across multiple chains and determining how settlement syncs without fragmentation.

7 Implementation and Adoption Strategy

7.1 OCP's Open-Source Model

- Not a company, not a closed system—OCP is a free, open-source standard.
- Already in production, tracking over $1B in private assets.

7.2 What's Next?

- Further adoption among issuers, broker-dealers, and DeFi protocols.
- Potential token model (TBD) to incentivize network effects.

8 Conclusion

Call to Action:

- OCP is live—join the movement to bring securities fully on-chain.