Perpetual Rates: A Mathematical Framework for Continuous-Tenor Interest Rate Swaps On-Chain

The CIRCA Protocol (Continuous Interest Rate Curve Architecture)

Jacob M. Boersma

Working Paper — Draft v0.3, July 8, 2026

***Abstract*— The interest rate swap is the largest single derivatives market in the world by notional outstanding, with ~$539 trillion in open contracts as of mid-2025. Its market structure has remained largely unchanged for four decades: bilaterally documented under ISDA, cleared through a small number of central counterparties, and organized around a discrete set of benchmark tenors that fragments duration management for participants requiring exposures between standard points. This paper presents CIRCA, a mathematical framework for implementing interest rate swaps on blockchain infrastructure that improves on the TradFi equivalent along four provable dimensions.**

First, we replace fixed-maturity settlement with a perpetual funding mechanism and prove that the resulting instrument's carry stream is economically equivalent to that of a continuously-rolled fixed-maturity IRS, with discretization errors bounded at 0.72 basis points per year under 8-hour funding intervals — empirically validated across the complete published history of the Secured Overnight Financing Rate. Second, we introduce a continuous tenor parameter realized through cubic spline interpolation across 15 anchor points spanning 1 month to 30 years, with maximum interpolation error of 0.052 basis points — approximately 673 times smaller than the duration approximation error TradFi participants routinely accept for off-benchmark tenor targets. Third, we prove the persistent duration property: CIRCA positions carry constant DV01 in time, delivered through a linear mark normalization, eliminating the rolling requirement that fixed-maturity instruments impose on participants seeking persistent rate exposure. Fourth, we develop a DV01-weighted unified liquidity pool and prove that it requires 15–40% less capital than fragmented per-tenor alternatives under the empirically calibrated cross-tenor correlation structure of SOFR rates.

We additionally derive a closed-form bound on the profit extractable by manipulating the on-chain rate curve: the bound is quadratic in the attacker's permitted position size and inversely proportional to both the market depth of the underlying rate instruments and the TWAP window length, and under the proposed protocol parameters it falls roughly two orders of magnitude below the fixed costs of mounting an attack. The framework is platform-agnostic; we evaluate four deployment targets (EVM-native, HyperCore via HIP-3, application-specific blockchain, and TradFi hybrid) with honest tradeoff assessment for each. We close with a precise enumeration of the framework's limitations — including zero convexity, the legal enforceability gap, and regulatory capital treatment — that future work must address.

The contribution of this paper is not a finished product but a specification rigorous enough to be built upon, examined, criticized, and extended. The continuous tenor parameter and the persistent duration property are not incremental improvements on the TradFi IRS; they are new financial capabilities that did not previously exist.

***Index Terms*—interest rate swaps, decentralized finance, blockchain, on-chain derivatives, term structure modeling, oracle design, market microstructure**

I. Motivation and Gap Analysis

A. The Interest Rate Swap as Financial Infrastructure

The interest rate swap is among the most important financial instruments ever devised. At its core, an IRS is structurally simple: two counterparties exchange a fixed stream of cash flows for a floating stream over a defined period, with payments netted against a notional principal that never changes hands. This simplicity belies an extraordinary range of applications. A corporate treasurer uses an IRS to convert floating-rate debt to fixed, achieving predictable financing costs. A pension fund uses one to align the duration of its assets with the known duration of its liabilities. A bank uses a portfolio of swaps to manage the mismatch between its fixed-rate mortgage book and its floating-rate deposit base. A hedge fund uses them to express directional views on the shape of the yield curve without taking on credit risk.

The scale of the market that has grown around this instrument is difficult to overstate. As of mid-2025, interest rate swaps outstanding totaled ~$539 trillion in notional — representing 81% of all interest rate derivatives and exceeding global GDP by a factor of approximately five [1], [2]. Daily turnover in overnight index swaps alone reached ~$5.1 trillion in April 2025. The IRS market is not peripheral to the global financial system. It is one of the mechanisms by which the global financial system manages its most fundamental risk: uncertainty about the future path of interest rates.

Despite this scale, the interest rate swap market has a structural architecture that has remained largely unchanged since its emergence in the early 1980s. Positions are negotiated bilaterally or on regulated swap execution facilities, documented under International Swaps and Derivatives Association (ISDA) master agreements, and cleared through a small number of central counterparties — principally LCH SwapClear, which handles the majority of cleared IRS volume globally [4]. The rate benchmarks against which floating legs are priced — SOFR in US dollar markets following the LIBOR transition — are published by centralized administrators under regulatory oversight.

This architecture is robust, deeply liquid, and serves its participants well in many respects. It is also, as this paper argues, structurally limited in ways that blockchain-based infrastructure can improve upon in a mathematically precise and provably superior manner.

B. *Three Structural Limitations of TradFi Interest Rate Swaps*

1) The Discrete Tenor Problem: The IRS market organizes itself around a fixed set of benchmark tenors: 1-month, 3-month, 6-month, 1-year, 2-year, 3-year, 5-year, 7-year, 10-year, 15-year, 20-year, and 30-year. These tenors are liquid because market convention has made them liquid — they are the points at which dealers concentrate their quoting activity, clearinghouses design their margin models, and data vendors publish reference rates. Between these points, the market thins dramatically. A participant seeking a 3.7-year swap must negotiate a bespoke instrument with a dealer at a privately determined rate, or construct an approximation by combining the 3-year and 5-year benchmark instruments in proportions that target the desired duration.

The combination approach introduces a structural basis risk that is not present in the target exposure. Consider a portfolio manager targeting a duration of $D^* = 3.7$ years with notional $N =$ \$100M. Using the available 3-year and 5-year instruments:

$$w_{3Y} \cdot 3 + w_{5Y} \cdot 5 = 3.7, \quad w_{3Y} + w_{5Y} = 1$$

Solving: $w_{3Y} = 0.65$, $w_{5Y} = 0.35$. The manager must execute two positions — \$65M at 3 years and \$35M at 5 years — rather than one. This decomposition creates exposure to the 3-year/5-year spread — the difference in rate movements between the two tenor points — which has no relationship to the manager's actual objective. Under a 20 basis point steepening of the 3-to-5-year segment of the curve, the tracking error against a true 3.7-year position is:

$$\begin{aligned}\text{Tracking Error} &= \$35\text{M} \times 5 \times 20 \times 0.0001 \\ &\quad - \$100\text{M} \times 3.7 \times 20 \times 0.0001 \times w_{5Y,3.7} \\ &= \$350{,}000\end{aligned}$$

This $\$350{,}000$ annual tracking error is structural — it arises not from any model error or execution failure but from the market's inability to provide a continuous tenor parameter. It scales linearly with notional and with the magnitude of non-parallel curve moves, making it a persistent and material cost for any participant managing complex duration targets.

2) The Duration Decay Problem: A fixed-maturity IRS has a duration that declines monotonically as it ages. A 5-year swap entered today has a dollar value of a basis point (DV01) of approximately:

$$\text{DV01} = N \cdot \tau \cdot 0.0001 \cdot P(t_0, T)$$

where $P(t_0, T)$ is the discount factor from inception to maturity. After three years, the same swap has a DV01 corresponding to its remaining 2-year life — roughly 40% of its original rate sensitivity. A participant who wishes to maintain a constant 5-year duration exposure must roll the swap at maturity, re-entering a new 5-year instrument and incurring the associated transaction costs. For long-horizon duration management — pension funds, insurance companies, sovereign wealth funds — this rolling requirement represents a persistent operational burden and a recurring transaction cost with no economic purpose beyond maintaining a target that the instrument itself is designed to abandon.

The total cost of rolling a fixed-maturity IRS of tenor τ over a holding period T_H is:

$$C_{roll}(T_H) = N \cdot \frac{s}{2} \cdot \left\lfloor \frac{T_H}{\tau} \right\rfloor \cdot \tau \cdot 0.0001$$

where s is the bid-offer spread in basis points. For a 5-year swap with a 1 basis point spread maintained over a 20-year horizon, the roll cost on a \$100M position totals $\$40{,}000$ in direct transaction costs — modest in isolation but compounding across large books and multiple instruments into a significant drag on long-horizon performance.

3) The Opacity Problem: The price of an interest rate swap in TradFi is not publicly observable. The fixed rate offered by a dealer incorporates the mid-market rate, a bid-offer spread that varies by counterparty relationship and flow, a credit valuation adjustment (CVA) reflecting bilateral counterparty risk, and a funding valuation adjustment (FVA) reflecting the dealer's internal funding cost. None of these components are disclosed to the end user. A participant receiving a quote has no means of verifying whether the offered rate is fair beyond soliciting competing quotes — a process that is itself subject to information leakage and relationship management constraints.

This opacity is not incidental to the TradFi IRS market structure. It is the market structure. Dealer profitability in rates markets depends substantially on the bid-offer spread and on the information asymmetry between dealers who see aggregate flow and end users who see only their own trades. The LIBOR scandal — in which panel banks submitted rates that reflected their own financial interests rather than their true borrowing costs — was the most visible expression of a market structure in which rate-setting opacity creates incentives for manipulation. The SOFR transition addressed the manipulation problem by grounding the overnight rate in actual transaction data, but it did not address the opacity in the swap rates derived from it.

C. *What Blockchain Infrastructure Changes*

Blockchain-based financial infrastructure offers properties that are structurally distinct from TradFi market architecture in three relevant ways.

Programmable continuous settlement. A smart contract can execute financial logic — computing payment amounts, transferring assets, updating position state — at any frequency, continuously, without the operational constraints that make high-frequency settlement impractical in TradFi. Where TradFi IRS settle periodically because settlement requires operational coordination between counterparties, custodians, and clearing-houses, an on-chain equivalent can settle continuously because settlement is a deterministic function of contract state. This property is the foundation of the perpetual funding mechanism central to the CIRCA framework.

Deterministic public pricing. An on-chain rate curve constructed from observable market data via a defined, publicly auditable methodology produces rates that any participant can independently verify and reproduce. There are no private adjustments, no relationship-dependent spreads, no information asymmetry between participants with access to aggregate flow and those without. The price of a swap is a deterministic function of publicly observable state.

Arbitrary parameterization. A smart contract imposes no constraint on the parameters of the financial instruments it supports beyond the computational limits of the underlying platform. Where TradFi instrument parameters are constrained by market convention and liquidity concentration, an on-chain instrument can accept any parameter within a defined range — including a tenor parameter that is a continuous real-valued input rather than a selection from a discrete menu.

These three properties, taken together, suggest that a carefully designed on-chain IRS framework could eliminate the discrete tenor problem, the duration decay problem, and the opacity problem simultaneously — not by replicating TradFi structure in a new medium, but by exploiting the structural properties of programmable settlement to design a fundamentally different instrument.

D. Prior Work and Its Limitations

Several prior attempts have been made to bring interest rate derivatives on-chain. Their limitations are instructive.

Yield tokenization protocols — most notably Pendle Finance [19] — decompose yield-bearing assets into principal and yield components, creating instruments that bear economic similarity to fixed and floating rate exposure. Pendle's approach has demonstrated genuine market demand: its total value locked grew from under ˜$300 million in early 2024 to approximately ˜$9 billion by mid-2025 [6]. However, yield tokenization is not an interest rate swap. It operates on a single asset's own yield rather than on a reference rate curve, produces instruments that expire at a fixed maturity requiring active management, and does not permit any form of continuous tenor selection. It is a fixed-income product built around a single asset's cash flows, not a generalized rate derivatives framework.

Fixed-rate lending protocols — including Notional Finance [20] and Yield Protocol [21] — have created markets for fixed-rate borrowing and lending at discrete maturities. These protocols demonstrate that on-chain fixed rate markets are feasible, but they address the lending market rather than the derivatives market. A fixed-rate loan is not an interest rate swap — it lacks the bilateral cash flow exchange, the leverage, and the duration management properties that make IRS valuable.

Early IRS attempts — Swivel Finance, Element Finance, and Sense Finance [22] — attempted to construct more general interest rate derivative markets on-chain. All achieved limited adoption. The common failure modes were: inability to bootstrap two-sided liquidity without a dominant underlying asset, design for a rate environment that subsequently changed, and dependence on discrete tenor structures that replicated TradFi's limitations without the liquidity that makes those limitations acceptable in TradFi.

None of these prior approaches addressed the three structural limitations identified in Section 1.2. None proposed a continuous tenor parameter. None developed a perpetual funding mechanism to replace fixed-maturity settlement. None constructed an on-chain rate curve capable of pricing instruments across the full term structure. The CIRCA framework addresses all three.

E. Contributions of This Paper

This paper makes five principal contributions to the literature on on-chain financial infrastructure and interest rate derivatives.

Contribution 1 — The continuous tenor parameter. We prove that a cubic spline interpolation across 15 anchor points spanning the 1-month to 30-year range produces rates within 0.052 basis points of theoretical fair value at any tenor input — an error approximately 2,000 times smaller than the duration approximation error TradFi participants accept when using discrete tenor instruments.

Contribution 2 — The perpetual funding mechanism for IRS. We prove that a perpetual swap with continuous funding is economically equivalent to a continuously-rolled fixed-maturity IRS, with deviations bounded at 0.72 basis points per year under 8-hour funding intervals — validated empirically against the full published history of SOFR from April 2018 to April 2026, including the September 2019 repo market stress event.

Contribution 3 — The persistent duration property. We prove that the CIRCA perpetual IRS satisfies the persistent duration property — its DV01 is constant in time at $N \cdot \tau \cdot 0.0001$ — eliminating the duration decay problem that requires active rolling in fixed-maturity instruments. We characterize the zero-convexity profile of the perpetual IRS and derive the roll cost savings over realistic holding periods.

Contribution 4 — The DV01-weighted unified pool framework. We prove that DV01 aggregation across arbitrary continuous tenor positions is exact under parallel rate shifts and exact bucket-by-bucket under non-parallel shifts, and that a unified liquidity pool with DV01-weighted portfolio margining requires 15–40% less capital than fragmented per-tenor alternatives under empirically calibrated cross-tenor correlation.

Contribution 5 — Manipulation resistance of the on-chain rate curve. We develop a formal adversarial model for the CIRCA rate curve and derive a closed-form bound on extractable manipulation profit: the bound is quadratic in the attacker's permitted position size and inversely proportional to both the market depth of the underlying rate instruments and the TWAP window length. Under the proposed position caps and oracle parameters, the maximum extractable profit at the curve's weakest point falls roughly two orders of magnitude below the fixed costs of mounting the attack.

Together, these contributions establish that an on-chain interest rate swap framework can improve on the TradFi model in duration precision, roll cost, capital efficiency, and price transparency — with quantified margins derived from formal proofs and empirical validation. The paper does not claim that the CIRCA framework dominates TradFi IRS on all dimensions. Section 6 enumerates the open problems and limitations that remain, including legal enforceability, regulatory capital treatment, and near-term liquidity depth — areas where the existing TradFi infrastructure retains meaningful advantages that this paper does not attempt to dismiss.

F. Organization

The remainder of this paper is organized as follows. Section 2 presents the CIRCA model — the perpetual funding mechanism, the continuous tenor parameter, and the formal proof of economic equivalence with continuously-rolled fixed-maturity IRS. Section 3 develops the on-chain rate curve — the anchor point set, the cubic spline construction, the interpolation error bound, and the manipulation resistance analysis. Section 4 presents the risk model — the DV01 framework, portfolio aggregation, the unified pool capital efficiency proof, and the margin model. Section 5 provides implementation appendices describing how the CIRCA framework maps onto specific blockchain infrastructure, with honest assessment of the tradeoffs of each deployment target. Section 6 states the open problems — the dimensions on which the framework does not yet provide a complete solution and the research directions required to address them.

II. The CIRCA Model

A. Overview

The CIRCA framework replaces three design choices made by the TradFi IRS market — discrete tenor selection, fixed maturity settlement, and periodic cash flow exchange — with three alternatives that exploit the structural properties of programmable on-chain settlement: a continuous tenor parameter, a perpetual funding mechanism, and a DV01-weighted unified pool. This section develops the first two of these and proves their core mathematical properties. The third is developed in Section 4.

The central result of this section is that a CIRCA position held from t_0 to T is economically equivalent to a continuously-rolled fixed-maturity IRS of the same tenor, notional, and fixed rate over the same period — with deviations from this equivalence that are bounded, characterized, and shown to be economically negligible under empirically validated parameter choices.

B. Instrument Definition

A CIRCA position is defined by the following parameters, fixed immutably at inception:

Definition 2.1 *(CIRCA Position)***.** A CIRCA position is a tuple $\mathcal{P} = (N, d, K, \tau, t_0, \Delta, \mathcal{O})$ where:

- $N \in \mathbb{R}_{>0}$ is the **notional** — the reference principal against which cash flows are computed, never exchanged
- $d \in \{+1, -1\}$ is the **direction** — $d = +1$ denotes pay-fixed (long floating, short fixed); $d = -1$ denotes receive-fixed
- $K \in \mathbb{R}_{>0}$ is the **fixed rate**, expressed in decimal (e.g., 0.053 for 5.3%), agreed at position open and immutable thereafter
- $\tau \in [1/12, 30]$ is the **tenor**, expressed in years, a continuous real-valued parameter representing the participant's target duration exposure
- $t_0 \in \mathbb{R}_{>0}$ is the **inception timestamp** — the Unix timestamp at which the position becomes active
- $\Delta \in \mathbb{R}_{>0}$ is the **funding interval** in years — the period between consecutive funding settlements; the protocol standard is $\Delta = 1/1095$ (8 hours)
- $\mathcal{O}$ is the **rate oracle** — a function $\mathcal{O}(t, \tau) \to \mathbb{R}_{>0}$ returning the continuously published floating rate at time t for tenor τ, satisfying the properties defined in Section 3

A CIRCA position has no maturity date. It remains open until the participant voluntarily closes it or until a margin breach triggers liquidation. This perpetual structure is the defining property that distinguishes it from all prior on-chain IRS attempts and from TradFi fixed-maturity instruments.

Definition 2.2 *(Funding Payment)***.** At each funding settlement time $t_k = t_0 + k\Delta$ for $k = 1, 2, 3, \ldots$, the net funding payment to a pay-fixed position ($d = +1$) is:

$$F_k = N \cdot (K - \mathcal{O}(t_{k-1}, \tau)) \cdot \Delta$$

If $F_k > 0$, the position holder pays F_k to the pool. If $F_k < 0$, the pool pays $|F_k|$ to the position holder. For a receive-fixed position ($d = -1$), signs are reversed. Payments are denominated in the position's settlement currency, typically a USD-pegged stablecoin.

Remark 2.1. The floating rate $\mathcal{O}(t_{k-1}, \tau)$ is observed at the beginning of each funding interval and applied to that interval — analogous to the in-advance rate setting convention used in TradFi SOFR-linked instruments. The oracle rate is snapshotted at t_{k-1} and does not change during the interval $[t_{k-1}, t_k]$.

C. The Fixed Rate at Inception

The fixed rate K is not chosen arbitrarily by the participant. At position open, the protocol determines the fair fixed rate as the value that makes the expected present value of all future funding payments equal to zero — the par rate condition, exactly as in TradFi IRS.

Under risk-neutral pricing with the oracle rate as the floating reference:

$$K_{par}(\tau, t_0) = \mathcal{O}(t_0, \tau)$$

That is, the par fixed rate at inception equals the current oracle rate for the position's tenor. This is the discrete analogue of the TradFi par swap rate condition, which sets the fixed rate equal to the weighted average of forward rates over the swap's life. In the CIRCA framework, since the floating rate is always observed at the same tenor τ regardless of time elapsed, the par rate reduces to the current spot rate at τ.

The AMM mechanism through which positions are opened may offer a fixed rate that differs from K_{par} by the AMM spread σ_{AMM}:

$$K_{offer}(\tau, t_0) = \mathcal{O}(t_0, \tau) + \sigma_{AMM} \cdot d$$

where $\sigma_{AMM} > 0$ is the bid-offer half-spread. Participants opening pay-fixed positions transact at $K_{par} + \sigma_{AMM}$ (they pay a slightly higher fixed rate); receive-fixed participants transact at $K_{par} - \sigma_{AMM}$. The spread σ_{AMM} compensates the liquidity pool for providing the opposing side of the trade and is a function of pool state developed in Section 4.

D. The Perpetual Funding Mechanism: Continuous Limit

We now establish the fundamental equivalence result. Consider the total funding value received by a pay-fixed CIRCA position holder over a holding period $[t_0, T]$ with $n = (T - t_0)/\Delta$ funding intervals:

$$V_{CIRCA}(t_0, T) = \sum_{k=1}^{n} F_k = N \cdot \sum_{k=1}^{n} (K - \mathcal{O}(t_{k-1}, \tau)) \cdot \Delta$$

Taking the limit as $\Delta \to 0$ — continuous funding — the discrete sum converges to a Riemann integral:

$$\begin{aligned} \lim_{\Delta \to 0} V_{CIRCA}(t_0, T) &= N \cdot \int_{t_0}^{T} (K - \mathcal{O}(t, \tau))\, dt \\ &= N \cdot \left[K(T - t_0) - \int_{t_0}^{T} \mathcal{O}(t, \tau)\, dt \right] \end{aligned} \tag{2.1}$$

Now consider a fixed-maturity IRS with the same notional N, fixed rate K, and floating rate $\mathcal{O}(t, \tau)$, settled continuously. Its total cash flow over $[t_0, T]$ is:

$$V_{IRS}(t_0, T) = N \cdot \int_{t_0}^{T} (K - \mathcal{O}(t, \tau))\, dt \tag{2.2}$$

Equations (2.1) and (2.2) are identical. This establishes:

Theorem 2.1 *(Continuous Equivalence)***.** In the continuous funding limit, a CIRCA position with fixed rate K, notional N, and tenor τ, held from t_0 to T, produces funding cash flows identical to those of a fixed-maturity IRS with the same parameters over the same holding period:

$$\lim_{\Delta \to 0} V_{CIRCA}(t_0, T) = V_{IRS}(t_0, T)$$

Proof. Direct from equations (2.1) and (2.2), which are both equal to $N \cdot \int_{t_0}^{T} (K - \mathcal{O}(t, \tau))\, dt$. □

Remark 2.2 *(The Tenor Interpretation)***.** Theorem 2.1 establishes equivalence between the CIRCA position and a fixed-maturity IRS of duration $T - t_0$, not of duration τ. The tenor parameter τ does not define the duration of the CIRCA position — it defines which point on the rate curve the floating leg references. This distinction is fundamental and is developed fully in Section 2.6. The CIRCA position is not equivalent to a single τ-year fixed-maturity swap. It is equivalent to continuously rolling a τ-year fixed-maturity swap, as we now prove.

E. Equivalence to a Continuously-Rolled Fixed-Maturity IRS

The precise instrument that a CIRCA position replicates is a continuously-rolled fixed-maturity IRS of tenor τ — not a single instrument with maturity T, but a sequence of τ-year swaps entered and rolled without gap, each paying the fixed rate K agreed at t_0 and receiving the then-current τ-year floating rate.

Definition 2.3 *(Continuously-Rolled IRS)***.** A continuously-rolled fixed-maturity IRS with tenor τ, fixed rate K, and notional N, initiated at t_0 and maintained through T, produces at each instant $t \in [t_0, T]$ a cash flow rate of:

$$\frac{dV_{roll}}{dt} = N \cdot (K - r_{FWD}(t, \tau))$$

where $r_{FWD}(t, \tau)$ is the τ-year forward rate prevailing at time t — the rate on a new τ-year swap entered at t. Under the assumption that the oracle $\mathcal{O}(t, \tau)$ correctly reflects this forward rate, $r_{FWD}(t, \tau) = \mathcal{O}(t, \tau)$, and:

$$V_{roll}(t_0, T) = N \cdot \int_{t_0}^{T} (K - \mathcal{O}(t, \tau))\, dt = V_{CIRCA}(t_0, T) \tag{2.3}$$

Corollary 2.1. A CIRCA position is economically equivalent to a continuously-rolled fixed-maturity IRS of tenor τ, under the condition that the oracle rate $\mathcal{O}(t, \tau)$ correctly reflects the prevailing τ-year swap rate at each time t.

Corollary 2.1 characterizes the carry component of the CIRCA position — the funding stream. The capitalized revaluation component is supplied by the position mark introduced in Section 2.6, subject to the duration normalization discussed there; together the two components complete the description of the instrument's economics. The instrument is more useful than a single τ-year swap for duration management precisely because it maintains the τ-year rate reference indefinitely — a property formalized in Section 2.6.

F. The Persistent Duration Property

The persistent duration property is the most important structural advantage of the CIRCA instrument over fixed-maturity IRS. We state and prove it formally.

Definition 2.4 *(DV01)***.** The dollar value of a basis point (DV01) of a financial position at time t is:

$$\text{DV01}(t) = \left| \frac{\partial V}{\partial \epsilon} \right|_{\epsilon = 0}$$

where ϵ is a parallel shift of the rate curve in basis points and V is the mark-to-market value of the position.

Definition 2.5 *(Position Mark)***.** The *mark* of a CIRCA position at time t is:

$$M(t) = N \cdot d \cdot (\mathcal{O}(t, \tau) - K) \cdot \tau$$

Variation margin is settled on changes in the mark at each funding interval (Section 4.4.2). The total economic value received by the position holder over a holding period $[t_0, T]$ is the sum of the funding stream and the change in the mark:

$$V_{total}(t_0, T) = \sum_{k=1}^{n} F_k + M(T) - M(t_0)$$

with $M(t_0) = 0$ under the par condition $K = \mathcal{O}(t_0, \tau)$. The funding stream is the carry component of the instrument; the mark is the capitalized revaluation component.

Duration normalization. The mark is deliberately linear in the oracle rate, with the tenor τ as the dollar-duration scale factor and no discount factor. This is a normalization choice whose consequence against the TradFi benchmark should be stated precisely. A continuously-rolled TradFi τ-year par swap has dollar duration $N \cdot A(\tau)$, where $A(\tau) = (1 - e^{-r\tau})/r$ is the discounted annuity — a quantity that is rate-dependent and strictly less than τ. CIRCA normalizes the mark with the undiscounted scale factor τ instead. This is precisely what delivers an exact, rate-independent DV01 and the zero-convexity property (Remark 2.3); the cost is a deterministic scaling basis between a CIRCA position and the rolled TradFi swap, of ratio $\tau/A(\tau)$ — approximately 1.10 at $\tau = 5$ with $r = 4\%$, rising to approximately 1.72 at $\tau = 30$. A participant who requires the rolled swap's dollar duration rather than the normalized one scales notional by $A(\tau)/\tau$, a closed-form deterministic conversion. The normalization trades exact replication of the TradFi annuity for exactness of the risk framework.

Theorem 2.2 *(Persistent Duration Property)***.** For a CIRCA position with notional N and tenor τ, the DV01 is constant in time:

$$\text{DV01}_{CIRCA}(t) = N \cdot \tau \cdot 0.0001 \quad \forall\, t \geq t_0$$

Proof. Under a parallel shift of ϵ basis points applied to the entire rate curve at time t, the oracle rate at the position's tenor becomes $\mathcal{O}(t, \tau) + \epsilon \cdot 0.0001$, and the mark changes by:

$$\frac{\partial M}{\partial \epsilon} = N \cdot d \cdot \tau \cdot 0.0001$$

a change realized by the holder through variation margin. The funding payment over the current interval changes by $N \cdot 0.0001 \cdot \Delta$ — a transient flow effect of order Δ whose capitalized value over all future intervals is already reflected in the mark. The instantaneous rate sensitivity of the position is therefore $|\partial M/\partial\epsilon| = N \cdot \tau \cdot 0.0001$. This quantity is constant in t: the mark references the τ-tenor point of the curve at all times regardless of how long the position has been open, and the scale factor τ is fixed at inception. $\square$

Theorem 2.3 *(Duration Decay of Fixed-Maturity IRS)***.** For a fixed-maturity IRS with notional N, maturity T, and continuous compounding discount factor $P(t, T) = e^{-r(T-t)}$, the DV01 at time t is:

$$\text{DV01}_{IRS}(t) = N \cdot (T - t) \cdot 0.0001 \cdot e^{-r(T-t)}$$

This is strictly decreasing in t for $t < T$:

$$\frac{d}{dt}\text{DV01}_{IRS}(t) = -N \cdot 0.0001 \cdot e^{-r(T-t)}(1 - r(T - t)) < 0$$

for $T - t < 1/r$ — that is, whenever the remaining maturity is below $1/r$ years, approximately 25 years at current rates ($r \approx 4\%$). Since virtually all fixed-maturity IRS have remaining maturities below this threshold, the DV01 of a fixed-maturity IRS is monotonically declining over its practical life.

Corollary 2.2 *(Roll Cost Savings)***.** A participant maintaining a constant τ-year duration exposure over a holding period T_H using fixed-maturity IRS must roll the position $\lfloor T_H/\tau \rfloor$ times, incurring total transaction costs of:

$$C_{roll}(T_H) = N \cdot \frac{s}{2} \cdot \left\lfloor \frac{T_H}{\tau} \right\rfloor \cdot \tau \cdot 0.0001$$

where s is the bid-offer spread in basis points. The equivalent CIRCA position requires zero rolls. For a \$100M 5-year position with a 1 basis point bid-offer spread maintained over 20 years, $C_{roll} = \$40{,}000$ in direct transaction costs, plus the operational overhead and timing risk of managing four roll events.

Remark 2.3 *(Zero Convexity)***.** The CIRCA position has zero dollar convexity:

$$\frac{\partial^2 V_{CIRCA}}{\partial \epsilon^2} = 0$$

This follows directly from the linearity of both the funding payment and the position mark (Definition 2.5) in the oracle rate: the mark's scale factor τ is a constant fixed at inception and contains no discount factor, so the first derivative with respect to a rate shift is constant and the second derivative is identically zero. The practical implication is that the DV01 aggregation across a portfolio of CIRCA positions is exact — not a first-order approximation — for any magnitude of rate shift, parallel or otherwise. This property is exploited in the unified pool risk model of Section 4. It also means that participants who require positive convexity — for example, those hedging mortgage-backed securities — cannot replicate a positively convex position using CIRCA instruments alone. This is a limitation stated honestly in Section 6.

G. Deviations from Equivalence: Discrete Funding

Theorem 2.1 established equivalence in the continuous limit. Real implementations use discrete funding intervals $\Delta > 0$. We now bound the resulting approximation error.

Theorem 2.4 *(Discretization Error Bound)***.** For a CIRCA position with notional N, funding interval Δ, and oracle rate process $\mathcal{O}(t, \tau)$ with total variation $\text{TV}(\mathcal{O}, t_0, T) = \int_{t_0}^{T} |\dot{\mathcal{O}}(t, \tau)|\, dt$ over the holding period $[t_0, T]$, the discretization error satisfies:

$$|V_{CIRCA}(t_0, T) - V_{IRS}(t_0, T)| \leq N \cdot \frac{\Delta}{2} \cdot \text{TV}(\mathcal{O}, t_0, T) \quad (2.4)$$

Proof. The discrete sum $\sum_{k=1}^{n} f(t_{k-1})\Delta$ approximates the integral $\int_{t_0}^{T} f(t)\, dt$ for $f(t) = K - \mathcal{O}(t, \tau)$. By the standard

TABLE I: 95th Percentile Total Variation of SOFR (basis points)

Window	Low-Rate	Hiking	Plateau	Full History
1 Year	1,660	588	695	1,571
2 Years	2,354	683	1,139	2,240
3 Years	2,525	1,846	1,346	2,400
5 Years	—	3,189	3,024	3,156

TABLE II: Discretization Error Bound (bps/yr), $N = \$10$M, p95 Total Variation (Full History)

Δ	1 Year	2 Years	3 Years	5 Years
8-hour (1/1095 yr)	**0.72** ✓	**0.51** ✓	**0.37** ✓	**0.29** ✓
Daily (1/365 yr)	2.15	1.53	1.10	0.86 ✓
Weekly (1/52 yr)	15.11	10.77	7.69	6.07

error bound for the rectangle rule, the approximation error for a function with bounded variation satisfies $|\sum f(t_{k-1})\Delta - \int f\,dt| \leq (\Delta/2)\cdot \mathrm{TV}(f, t_0, T)$. Since K is constant, $\mathrm{TV}(f) = \mathrm{TV}(\mathcal{O})$, and the result follows after multiplying by N. □

Empirical Calibration. The bound in (2.4) depends on $\mathrm{TV}(\mathcal{O}, t_0, T)$ — the total variation of the floating rate over the holding period. We calibrate this using the complete published history of the Secured Overnight Financing Rate (SOFR) from April 3, 2018 to April 24, 2026, comprising 2,013 published business days sourced from the Federal Reserve Bank of St. Louis (FRED series: SOFR) [3].

The total variation is estimated empirically as $\mathrm{TV}(\mathcal{O}, t_0, T) \approx \sum_i |\mathcal{O}(t_i, \tau) - \mathcal{O}(t_{i-1}, \tau)|$ over rolling windows of 1, 2, 3, and 5 years. We stratify by three rate regimes that characterize the SOFR history: the low-rate period (April 2018 – February 2022), the Federal Reserve hiking cycle (March 2022 – July 2023), and the subsequent plateau (August 2023 – April 2026).

Table 2.1 reports the 95th percentile total variation across all rolling windows within each regime, expressed in basis points.

Note: The 5-year window has no observations in the low-rate regime because SOFR was first published in April 2018 and the regime ended in February 2022, a span of less than 5 years.

Note: The low-rate 1-year p95 of 1,660 bps is dominated by the September 17–18, 2019 repo market seizure, in which SOFR moved 282 basis points in a single day followed by 270 basis points the next — a technical liquidity event subsequently addressed by the Federal Reserve's standing repo facility and not indicative of ongoing rate volatility [7].

✓ *indicates bound below the 1.00 bps/yr materiality threshold.*

Corollary 2.3 *(Recommended Funding Interval)***.** The 8-hour funding interval is the largest interval satisfying the 1 bps/yr materiality threshold across all holding periods and rate regimes in the empirical sample. It is adopted as the CIRCA protocol standard. This bound holds under the most extreme rate dislocation in SOFR's published history; in normal rate environments, the realized error is substantially smaller.

Remark 2.4. The discretization error bound is independent of the notional N when expressed in basis points per year, and independent of the funding interval Δ in the absolute dollar sense for the compounding deviation analyzed in Section 2.8. These independence properties simplify the margin model of Section 4 by ensuring that discretization error does not scale with position size in the basis point sense.

H. Deviations from Equivalence: Compounding

A traditional IRS can be structured with compounding — net payments received at each settlement date earn interest at the reinvestment rate until maturity. The CIRCA funding mechanism does not compound: funding payments are transferred at each interval without accumulation. We bound this difference.

Theorem 2.5 *(Compounding Deviation Bound)***.** Let $\bar{r}$ denote the short-term reinvestment rate, $M = \max_{t\in[t_0,T]} |K - \mathcal{O}(t, \tau)|$ the maximum absolute net rate differential, and $T - t_0$ the holding period. The present value difference attributable to compounding between a CIRCA position and an equivalent compounding fixed-maturity IRS satisfies:

$$|\Gamma| \leq \frac{1}{2} \cdot N \cdot \bar{r} \cdot M \cdot (T - t_0)^2 \tag{2.5}$$

Under a mean-reverting rate process with annualized volatility σ_r, the expected compounding deviation satisfies:

$$\mathbb{E}[|\Gamma|] \approx \frac{2}{15} \cdot N \cdot \bar{r} \cdot \sigma_r \cdot (T - t_0)^{5/2} \tag{2.6}$$

Proof. The reinvestment gain on a single period's net payment $p_k = N(K - \mathcal{O}(t_{k-1}, \tau))\Delta$ held from t_k to T is $p_k \cdot \bar{r} \cdot (T - t_k)$ to first order in $\bar{r}\Delta$. Summing across all periods and bounding $|K - \mathcal{O}|$ by M yields (2.5). The expected value result (2.6) follows from the mean-reverting assumption, under which $\mathbb{E}[|K - \mathcal{O}(t, \tau)|] \approx \sigma_r\sqrt{t - t_0}$, integrated against the remaining time $(T - t)$ and evaluated in closed form as $\frac{4}{15}(T - t_0)^{5/2}$. □

Numerical Evaluation. For $N = \$10$M, $\bar{r} = 0.04$, $\sigma_r = 0.01$ (100 bps/yr), and $T - t_0 = 5$ years:

$$\mathbb{E}[|\Gamma|] \approx \frac{2}{15} \times 10{,}000{,}000 \times 0.04 \times 0.01 \times 5^{2.5} \approx \$14{,}900$$

This represents approximately 1.5 basis points per year on a \$10M position — below transaction costs for any institutional IRS trade and below the discretization error bound established in Theorem 2.4. The compounding deviation is therefore not a material source of difference between the CIRCA instrument and its TradFi equivalent.

Remark 2.5. Equations (2.5) and (2.6) are both independent of the funding interval Δ. The compounding deviation is a function of the holding period and rate environment, not of how frequently funding is exchanged. This confirms that the choice of funding interval in Section 2.7 does not affect the compounding deviation — the two error sources are orthogonal.

I. Summary of Section 2

The CIRCA position is formally defined as a perpetual instrument with a continuous tenor parameter, a fixed rate locked at inception, and a floating rate continuously observed from the on-chain rate curve at the position's tenor. The following results have been established:

Result 2.1. In the continuous funding limit, the funding stream of a CIRCA position produces cash flows identical to those of a fixed-maturity IRS over the same holding period (Theorem 2.1).

Result 2.2. A CIRCA position is economically equivalent to a continuously-rolled fixed-maturity IRS of tenor τ — not a single τ-year instrument, but a continuously maintained τ-year rate exposure (Corollary 2.1).

Result 2.3. The DV01 of a CIRCA position is constant in time at $N \cdot \tau \cdot 0.0001$, satisfying the persistent duration property; the property is delivered through the linear mark normalization of Definition 2.5. The DV01 of a fixed-maturity IRS declines monotonically to zero at maturity (Theorems 2.2 and 2.3).

Result 2.4. The discretization error from 8-hour funding intervals is bounded at 0.72 bps/yr under the 95th percentile historical SOFR total variation, empirically validated across April 2018 – April 2026 including the September 2019 repo market stress event (Theorem 2.4, Table 2.2).

Result 2.5. The compounding deviation between the CIRCA instrument and a compounding IRS is bounded at approximately 1.5 bps/yr in expectation under realistic rate dynamics, independent of the funding interval (Theorem 2.5).

Together, these results establish that the CIRCA perpetual IRS is a well-defined financial instrument with a precise relationship to its TradFi equivalent and with deviations from that equivalence that are bounded, characterized, and economically negligible.

III. The CIRCA Rate Curve

A. Overview

Section 2 treated the oracle $\mathcal{O}(t, \tau)$ as a function satisfying certain properties without specifying its construction. This section opens that black box. The CIRCA rate curve is an on-chain cubic spline constructed from 15 anchor points spanning the 1-month to 30-year tenor range. It is the mechanism by which the continuous tenor parameter of Section 2 is realized: given any $\tau \in [1/12, 30]$, the curve returns a rate $\mathcal{O}(t, \tau)$ that is within a formally bounded error of the theoretical fair rate at that tenor.

This section makes three contributions. First, it specifies the anchor point set and the two-zone density design that balances accuracy against oracle update cost. Second, it proves that the cubic spline interpolation error is bounded at 0.052 basis points across the full supported tenor range — a bound approximately 2,000 times smaller than the duration approximation error TradFi participants accept as standard. Third, it establishes a formal adversarial model for the rate curve and derives the manipulation profit bound: the maximum profit extractable by distorting the curve is quadratic in the attacker's permitted position size and inversely proportional to both the market depth of the underlying rate instruments and the length of the TWAP window — and, under the proposed protocol parameters, falls roughly two orders of magnitude below the fixed costs of mounting an attack.

B. The Anchor Point Set

The rate curve is anchored at 15 tenor points, organized into two density zones reflecting the distinct behavior of the yield curve at short and long maturities.

Definition 3.1 *(Anchor Point Set)***.** The CIRCA anchor point set is:

$$\mathcal{T} = \{T_1, T_2, \ldots, T_{15}\}$$

with the following elements, expressed in years:

$$\mathcal{T}_{short} = \left\{ \frac{1}{365}, \frac{1}{12}, \frac{3}{12}, \frac{6}{12}, \frac{9}{12}, 1, \frac{3}{2} \right\}$$

$$\mathcal{T}_{long} = \{2, 3, 5, 7, 10, 15, 20, 30\}$$

$$\mathcal{T} = \mathcal{T}_{short} \cup \mathcal{T}_{long}$$

where the elements of $\mathcal{T}_{short}$ correspond to overnight, 1-month, 3-month, 6-month, 9-month, 1-year, and 18-month tenors, and the elements of $\mathcal{T}_{long}$ correspond to 2-year through 30-year tenors at the standard TradFi benchmark points.

The minimum supported position tenor is $\tau_{min} = 1/12$ (1 month). The overnight anchor point $T_1 = 1/365$ is included to constrain the short end of the spline and to anchor the curve's behavior near zero — it is not a valid position tenor. The maximum supported position tenor is $\tau_{max} = 30$ years, corresponding to the outer boundary of liquid SOFR swap markets.

Rationale for Two-Zone Density. The short end of the yield curve is characterized by step-function dynamics: rates are stable between Federal Open Market Committee (FOMC) meetings and move discontinuously at policy announcements. Capturing this behavior accurately requires dense anchor points in the sub-2-year range. The long end of the curve is smoother — rates are driven by term premium dynamics that evolve gradually — and requires fewer anchor points for equivalent interpolation accuracy. The two-zone design allocates seven anchors to cover 0-18 months and eight anchors to cover 2-30 years, reflecting this asymmetry.

Anchor Rate Sources. Each anchor rate $r_i = \mathcal{O}(t, T_i)$ is sourced from the most liquid observable instrument at that tenor:

The oracle aggregates prices from multiple independent data sources for each anchor and computes a time-weighted average price (TWAP) over a governance-specified window W. The TWAP design is specified in Section 3.5.

TABLE III: Anchor Rate Sources

Anchor	Tenor	Source Instrument
T_1	Overnight	SOFR overnight fixing (NY Fed)
T_2	1-month	SOFR futures (SR1, front contract)
T_3	3-month	SOFR futures (SR1, 3-month implied)
T_4	6-month	SOFR futures (SR3, 6-month implied)
T_5	9-month	SOFR futures (SR3, 9-month implied)
T_6	1-year	SOFR OIS swap rate
T_7	18-month	SOFR OIS swap rate
T_8–T_{15}	2Y–30Y	SOFR swap rates (ICE Swap Rate or equivalent)

C. The Cubic Spline Construction

Definition 3.2 *(Natural Cubic Spline)***.** Given the anchor point set $\mathcal{T} = \{T_1 < T_2 < \cdots < T_{15}\}$ and corresponding anchor rates $\mathbf{r} = \{r_1, r_2, \ldots, r_{15}\}$, the CIRCA rate curve $S : [T_1, T_{15}] \to \mathbb{R}$ is the unique natural cubic spline satisfying:

(i) **Interpolation:** $S(T_i) = r_i$ for all $i = 1, \ldots, 15$

(ii) **Piecewise cubic:** On each interval $[T_i, T_{i+1}]$, S coincides with a cubic polynomial $S_i(\tau) = a_i + b_i(\tau - T_i) + c_i(\tau - T_i)^2 + d_i(\tau - T_i)^3$

(iii) C^2 **continuity:** S, S', and S'' are continuous at all interior knots $T_2, \ldots, T_{14}$

(iv) **Natural boundary conditions:** $S''(T_1) = S''(T_{15}) = 0$

The natural boundary condition imposes that the curve is linear (zero curvature) at the endpoints. This is appropriate for a yield curve: the overnight rate is determined by monetary policy and has no curvature, and the 30-year rate is at the outer boundary of liquid markets where extrapolation assumptions should be minimal.

Coefficient Computation. The spline coefficients $\{a_i, b_i, c_i, d_i\}_{i=1}^{14}$ are uniquely determined by the anchor rates $\mathbf{r}$ via the standard tridiagonal system. Define the interval widths $h_i = T_{i+1} - T_i$. The second derivatives $M_i = S''(T_i)$ satisfy the linear system:

$$
\begin{aligned}
h_{i-1}M_{i-1} + 2(h_{i-1} + h_i)M_i + h_i M_{i+1} \\
= 6\left(\frac{r_{i+1} - r_i}{h_i} - \frac{r_i - r_{i-1}}{h_{i-1}}\right)
\end{aligned}
$$

for $i = 2, \ldots, 14$, with boundary conditions $M_1 = M_{15} = 0$. This system is tridiagonal and strictly diagonally dominant, guaranteeing a unique solution computable in $O(n)$ operations via the Thomas algorithm. The remaining coefficients are recovered as:

$$
\begin{aligned}
a_i = r_i, \quad d_i = \frac{M_{i+1} - M_i}{6h_i}, \quad c_i = \frac{M_i}{2}, \\
b_i = \frac{r_{i+1} - r_i}{h_i} - \frac{h_i(2M_i + M_{i+1})}{6}
\end{aligned}
$$

On-Chain Implementation. The 56 spline coefficients $\{a_i, b_i, c_i, d_i\}_{i=1}^{14}$ are stored on-chain in a fixed-size array updated atomically whenever the oracle publishes new anchor rates. Rate evaluation at any tenor $\tau \in [T_i, T_{i+1}]$ requires: (1) identifying the interval containing τ via binary search over $\mathcal{T}$ in $O(\log 15) = O(1)$ operations, and (2) evaluating the cubic polynomial $S_i(\tau)$ via Horner's method in 4 multiplications and 4 additions. The total gas cost of a rate query is dominated by the binary search and is negligible relative to the cost of a funding settlement transaction.

Remark 3.1 *(Fixed-Point Arithmetic)***.** Solidity operates on integer arithmetic with no native floating-point support. Spline coefficients and rate values are stored as fixed-point numbers with 18 decimal places of precision (consistent with ERC-20 token conventions), using an established fixed-point arithmetic library. The rounding error introduced by 18-decimal fixed-point representation is bounded at 10^{-18} per arithmetic operation — negligible relative to the interpolation error bound established in Theorem 3.1.

D. The Interpolation Error Bound

Theorem 3.1 *(Spline Interpolation Error Bound)***.** Let $r : [T_1, T_{15}] \to \mathbb{R}$ denote the true theoretical rate curve and S the natural cubic spline of Definition 3.2. For any yield curve consistent with the Nelson-Siegel family of term structure models with parameters in the historically observed range, the pointwise interpolation error satisfies:

$$
\begin{aligned}
|r(\tau) - S(\tau)| &\le \frac{h_i^4}{384} \cdot \max_{\xi \in [T_i, T_{i+1}]} |r^{(4)}(\xi)| \\
&\le \epsilon_{spline}(\tau) \le 0.052 \text{ bps} \quad \forall \tau \in [1/12, 30]
\end{aligned}
$$

where $h_i = T_{i+1} - T_i$ is the width of the interval containing τ, and $r^{(4)}$ denotes the fourth derivative of the true rate curve with respect to tenor.

Proof. The error bound for natural cubic spline interpolation on an interval $[T_i, T_{i+1}]$ is the classical result:

$$
|r(\tau) - S(\tau)| \le \frac{h_i^4}{384} \cdot \max_{\xi \in [T_i, T_{i+1}]} |r^{(4)}(\xi)| \tag{3.1}
$$

It remains to bound $|r^{(4)}(\xi)|$. We use the Nelson-Siegel model [9] as the reference yield curve family, as it is the most widely adopted parsimonious model among central banks and academic researchers and provides a conservative upper bound on fourth-derivative magnitude. The Nelson-Siegel rate function is:

$$
r(\tau) = \beta_0 + \beta_1 \cdot \frac{1 - e^{-\lambda\tau}}{\lambda\tau} + \beta_2 \cdot \left(\frac{1 - e^{-\lambda\tau}}{\lambda\tau} - e^{-\lambda\tau}\right) \tag{3.2}
$$

with decay parameter $\lambda > 0$ and level, slope, and curvature factors $\beta_0, \beta_1, \beta_2$. The fourth derivative of r with respect to τ satisfies:

$$
|r^{(4)}(\tau)| \le \lambda^4 \cdot (|\beta_1| + 2|\beta_2|) \cdot e^{-\lambda\tau} \tag{3.3}
$$

Using a decay parameter consistent with Diebold and Li [10], $\lambda = 0.0609$, and curvature/slope bounds $|\beta_i| \le 0.05$ for all i — a conservative bound consistent with common implementation practice for calibrating the model to historically observed U.S. rate curves, rather than a figure drawn from a single official methodological source. These bounds

TABLE IV: Interpolation Error Bound by Interval

Interval	h (years)	ϵ_{spline} (bps)
ON – 1M	0.082	< 0.000001
1M – 3M	0.167	< 0.000001
3M – 6M	0.250	< 0.000001
6M – 9M	0.250	< 0.000001
9M – 1Y	0.250	< 0.000001
1Y – 18M	0.500	< 0.00002
18M – 2Y	0.500	< 0.00002
2Y – 3Y	1.000	< 0.0003
3Y – 5Y	2.000	< 0.005
5Y – 7Y	2.000	< 0.005
7Y – 10Y	3.000	< 0.025
10Y – 15Y	5.000	< 0.162
15Y – 20Y	5.000	< 0.162
20Y – 30Y	**10.000**	< 0.052

are conservative — they correspond to a steeply curved yield curve in a high-rate environment. Substituting:

$$\max_{\tau} |r^{(4)}(\tau)| \leq (0.0609)^4 \times 0.15 \times 1 \approx 2.0 \times 10^{-5} \text{ per year}^4$$

The maximum interpolation error is achieved at the widest interval. In the anchor set $\mathcal{T}$, the widest interval is $[T_{14}, T_{15}] = [20, 30]$ with $h_{14} = 10$ years:

$$\epsilon_{spline}^{max} = \frac{10^4}{384} \times 2.0 \times 10^{-5} = 26.04 \times 2.0 \times 10^{-5} \approx 5.2 \times 10^{-4}$$

Converting to basis points: $\epsilon_{spline}^{max} \approx 0.052$ bps. □

Note: The 20Y–30Y interval has the largest h but the smallest $|r^{(4)}|$ because the long end of the yield curve is extremely flat — the exponential decay in equation (3.3) renders the fourth derivative near zero for large τ. The practical worst case is the 10Y–20Y range where curvature persists and intervals are moderately wide, yielding a maximum of 0.162 bps.

Corollary 3.1 *(Comparison to TradFi Duration Approximation Error)***.** The maximum interpolation error of 0.052 basis points (or 0.162 bps in the 10Y–20Y range) is to be compared against the duration approximation error that TradFi participants accept as a matter of standard practice. For a target duration $D^* = 3.7$ years lying between the TradFi 3-year and 5-year benchmark tenors, the tracking error on a \$100M portfolio under a 20 basis point curve steepening is \$350,000 per year (derived in Section 1.2.1). The equivalent tracking error from spline interpolation error on the same portfolio is:

$$\begin{aligned} \text{Tracking Error}^{spline} &= \$100\text{M} \times \epsilon_{spline}^{max} \times 0.0001 \\ &= \$100\text{M} \times 5.2 \times 10^{-6} = \$520 \text{ per year} \end{aligned}$$

The ratio is:

$$\frac{\text{Tracking Error}^{TradFi}}{\text{Tracking Error}^{spline}} = \frac{\$350{,}000}{\$520} \approx 673\times$$

The spline interpolation error introduces tracking error approximately 673 times smaller than the duration approximation error TradFi participants routinely accept. For positions in the 10Y–20Y range where the interpolation error is largest, this ratio narrows to approximately 130 times — still three orders of magnitude superior.

Remark 3.2 *(Anchor Point Adequacy)***.** Theorem 3.1 establishes that 15 anchor points are sufficient for the stated error bound. Adding more anchor points would improve the bound further — the error scales as h^4, so halving the widest interval width reduces the maximum error by a factor of 16. However, each additional anchor point increases oracle update cost and governance complexity. The current 15-point set represents the minimum anchor density required to achieve the stated bound across the full tenor range under historically calibrated curve shapes.

E. Oracle Design and TWAP Windowing

The spline is only as reliable as the anchor rates that define it. This section specifies the oracle mechanism that produces anchor rates with formal staleness and manipulation resistance properties.

Definition 3.3 *(CIRCA Rate Oracle)***.** The CIRCA rate oracle is a smart contract function $\mathcal{O} : \mathbb{R}_{\geq 0} \times [1/12, 30] \to \mathbb{R}_{>0}$ satisfying:

(i) **Currency:** For each anchor $T_i \in \mathcal{T}$, the oracle maintains a TWAP computed over a window of length W (governance parameter; proposed minimum: $W = 1$ hour for short end, $W = 24$ hours for long end): $\mathcal{O}(t, T_i) = \frac{1}{W} \int_{t-W}^{t} p_i(s)\, ds$ where $p_i(s)$ is the volume-weighted mid-price of the source instrument at time s

(ii) **Interpolation:** For $\tau \in [T_i, T_{i+1}]$, $\mathcal{O}(t, \tau) = S_i(\tau)$ where S is the current spline computed from anchor rates $\{\mathcal{O}(t, T_j)\}_{j=1}^{15}$

(iii) **Staleness:** The oracle is considered stale at anchor T_i if no source price has been observed within the staleness window W_s (proposed: $W_s = 25$ hours, to accommodate weekends and US bank holidays for SOFR-sourced anchors). A stale oracle does not update $\mathcal{O}(t, T_i)$ — it holds the last valid value and emits a staleness event

(iv) **Multi-source aggregation:** Each anchor rate is computed as the median of at least three independent data sources to prevent single-source manipulation. Sources are weighted by their historical accuracy relative to subsequent realized rates

Remark 3.3 *(TWAP Window Asymmetry)***.** The proposed TWAP window is asymmetric across the curve — shorter at the short end ($W = 1$ hour) and longer at the long end ($W = 24$ hours). This reflects the different liquidity profiles of the underlying instruments. SOFR futures trade continuously with deep intraday liquidity — a 1-hour TWAP captures sufficient volume for manipulation resistance. Long-dated swap rates are quoted less frequently and with wider intraday spreads — a 24-hour TWAP is necessary to average over sufficient transactions. The asymmetric design minimizes staleness risk at the short end (which changes frequently due to FOMC dynamics) while maximizing manipulation resistance at the long end (which is cheaper to manipulate due to lower market depth).

F. Manipulation Resistance

We now develop the formal adversarial model for the CIRCA rate curve and derive the bound on extractable manipulation profit.

Definition 3.4 *(Adversarial Model)***.** An adversary $\mathcal{A}$ has the following capabilities:

- $\mathcal{A}$ can trade in any underlying rate market — SOFR futures, OIS swap markets, Treasury markets — in unlimited size subject to market impact
- $\mathcal{A}$ can open CIRCA positions of any notional subject to the protocol's margin requirements
- $\mathcal{A}$ cannot alter the spline computation, the TWAP mechanism, or the on-chain settlement logic
- $\mathcal{A}$ cannot prevent other participants from trading

The adversary's objective is to open CIRCA positions at a manipulated rate, then allow the oracle to revert to fair value and realize — through the mark and the excess funding stream — the difference between the manipulated fixed rate and fair value.

Definition 3.5 *(Market Depth)***.** The market depth D_k at anchor T_k is the trading notional required to displace the rate at that anchor by one basis point and sustain the displacement for one trading day against mean-reverting flow:

$$D_k = \frac{\text{Daily Volume}_k}{\text{Daily Rate Volatility}_k \text{ (bps)}}$$

Table 3.2 reports estimated market depth by anchor tenor based on BIS [1] and CME published volume data.

The 30-year anchor is the least liquid and therefore the cheapest to manipulate — it is the binding constraint for manipulation resistance and the focus of the analysis below.

Theorem 3.2 *(Manipulation Profit Bound)***.** Let δ denote the magnitude of a sustained distortion at anchor T_k in basis points, D_k the market depth (Definition 3.5), w the TWAP window length expressed in trading days, and $c \in [1/2, 1]$ the round-trip loss fraction on manipulative flow. Let ADV01 denote the aggregate dollar duration (in dollars per basis point) of the attack positions opened against the distorted curve. The attacker's net profit satisfies:

$$\Pi_{net}(\delta) \leq \text{ADV01} \cdot \delta \; - \; c \cdot \delta^2 \cdot 0.0001 \cdot D_k \cdot w \qquad (3.4)$$

and the maximum extractable profit, optimizing over δ, is:

$$\Pi_{max} = \frac{\text{ADV01}^2}{4c \cdot 0.0001 \cdot D_k \cdot w}, \quad \text{achieved at } \delta^* = \frac{\text{ADV01}}{2c \cdot 0.0001 \cdot D_k \cdot w} \qquad (3.5)$$

Proof. **Profit.** A position opened against a curve distorted by $\delta_{spline}(\tau) \leq \delta$ basis points (Theorem 3.3) locks a fixed rate mispriced by at most δ relative to fair value. When the oracle reverts, the holder realizes the capitalized value of the mispricing through the mark (Definition 2.5): the mark gain is at most $N \cdot \tau \cdot 0.0001 \cdot \delta = \text{DV01} \cdot \delta$ per position, or $\text{ADV01} \cdot \delta$ in aggregate. The same value accrues as excess funding over time if the position is held rather than closed; the two are equivalent in present-value terms, and the mark realization is immediate, so the capitalized expression is the binding bound. Critically, this profit is independent of the TWAP window: the locked fixed rate is immutable, so the mispricing persists for the life of the position regardless of how quickly the published curve reverts.

Cost. Sustaining a δ basis point displacement of the source instrument against mean-reverting market flow requires absorbing opposing volume of approximately $\delta \cdot D_k$ in notional per trading day, or $\delta \cdot D_k \cdot w$ over the TWAP window. The attacker's round-trip loss on this flow — acquiring at displaced prices and unwinding at reverted prices — is approximately $c \cdot \delta \cdot 0.0001$ per dollar of notional traded, giving total cost $c \cdot \delta^2 \cdot 0.0001 \cdot D_k \cdot w$. The cost is quadratic in δ because the required volume and the per-dollar loss each scale linearly with the displacement.

Maximizing the concave quadratic $\Pi_{net}(\delta)$ over δ yields the stated δ^* and Π_{max}. ☐

Remark 3.4 *(The Role of the TWAP Window and Position Caps)***.** Two consequences of equation (3.5) determine the protocol's defensive design. First, the TWAP window enters the maximum extractable profit inversely: $\Pi_{max} \propto 1/w$, so doubling the window halves the attacker's ceiling. This is the formal justification for the asymmetric TWAP design of Section 3.5 — the long end, where market depth is thinnest, carries the longest window, compounding the defense precisely where it is most needed. Second, Π_{max} is quadratic in ADV01: per-tenor-bucket DV01 caps reduce the attacker's ceiling quadratically, so halving the cap quarters the maximum extractable profit. Position caps are therefore not a supplementary defense layer — together with underlying market depth and the TWAP window, they are the primary determinants of the attack's economics.

Corollary 3.2 *(Numerical Bound at the Weakest Anchor)***.** Evaluate at the least liquid anchor (30-year) using the conservative lower-bound depth $D_{30Y} = \$3.3\text{B}$ per basis point, a 24-hour TWAP spanning $w = 3$ trading days of underlying market hours, $c = 1/2$, and a bucket cap of \$50,000 of DV01 per tenor bucket (corresponding to \$500M of DV01-weighted notional):

$$\delta^* = \frac{50{,}000}{2 \cdot 0.5 \cdot 0.0001 \cdot 3.3 \times 10^9 \cdot 3} \approx 0.05 \text{ bps},$$
$$\Pi_{max} = \frac{(50{,}000)^2}{4 \cdot 0.5 \cdot 0.0001 \cdot 3.3 \times 10^9 \cdot 3} \approx \$1{,}260$$

The optimal attack distorts the 30-year anchor by five hundredths of a basis point and extracts at most approximately \$1,260 — before the fixed costs of mounting it. Opening attack positions at the bucket cap incurs AMM spread and protocol fees on the order of $\$10^5$, and the manipulative flow itself requires deploying approximately $\delta^* \cdot D_{30Y} \cdot w \approx \$500\text{M}$ of trading notional with its associated margin and execution costs. The attack is unprofitable by roughly two orders of magnitude at the weakest point on the curve; at shorter tenors, market

TABLE V: Estimated Market Depth by Anchor Tenor

Anchor	Daily Volume	Daily Volatility	D_k (\$/bps)
Overnight	\$1–4T\$	1 bps	$\sim$ \$1–4T
1M–3M (SOFR futures)	500B–2T	2 bps	$\sim$ \$250B–1T
6M–12M (SOFR futures)	200B–800B	3 bps	$\sim$ \$67B–267B
2Y–5Y (SOFR swaps)	100B–500B	3 bps	$\sim$ \$33B–167B
7Y–10Y (SOFR swaps)	50B–200B	3 bps	$\sim$ \$17B–67B
15Y–20Y (SOFR swaps)	10B–50B	3 bps	$\sim$ \$3.3B–17B
30Y (SOFR swaps)	5**B–**20**B**	**3 bps**	$\sim$ \$1.7**B–**6.7**B**

depth is one to three orders of magnitude greater and the bound tightens proportionally.

Theorem 3.3 *(Spline Locality Limits Contagion)***.** A manipulation of anchor T_k by δ_k basis points distorts the interpolated rate at tenor τ by at most $|B_k(\tau)| \cdot \delta_k$ basis points, where $B_k(\tau)$ is the k-th cubic spline basis function. For tenors more than one interval removed from T_k:

$$|B_k(\tau)| < \epsilon_{basis} \ll 1$$

Proof. The cubic spline basis functions have local support — the influence of knot k decays rapidly beyond adjacent intervals by the C^2 continuity conditions. The precise decay rate depends on the interval widths but for the CIRCA anchor set, the basis function value at a tenor two intervals removed from the manipulated knot is bounded by 10^{-3} — rendering cross-tenor contamination from a single-knot attack negligible. □

Corollary 3.3 *(Multi-Anchor Attack Cost)***.** To distort the rate curve uniformly by δ basis points across the full tenor range $[1/12, 30]$, an adversary must manipulate all 15 anchor points simultaneously, incurring total attack cost:

$$C_{total} = \delta \cdot 0.0001 \cdot \sum_{k=1}^{15} D_k \cdot w \gg \delta \cdot D_{30Y} \cdot w \cdot 0.0001$$

The total cost of a full-curve manipulation is dominated by the sum of market depths across all anchors — an amount vastly exceeding the cost of the single weakest-link attack. Multi-anchor attacks are therefore strictly more expensive than single-anchor attacks without producing proportionally larger profits, due to the locality property of Theorem 3.3.

G. FOMC Jump Handling

The CIRCA rate curve must correctly handle the discrete jumps in the short end of the yield curve that occur at FOMC policy announcements. Failing to account for these jumps would cause the short end of the spline to misrepresent market expectations between announcement dates.

Definition 3.6 *(FOMC-Adjusted Short End)***.** For tenor $\tau \in [T_1, T_7]$ (overnight to 18 months), the oracle incorporates a piecewise-constant step function for the expected policy rate path:

$$\mathcal{O}_{policy}(t, \tau) = \frac{1}{\tau} \sum_{j: t_j^{FOMC} \leq t+\tau} \Delta r_j^{FOMC} \cdot (t + \tau - t_j^{FOMC})$$

where t_j^{FOMC} are the FOMC meeting dates and Δr_j^{FOMC} are the market-implied rate changes at each meeting, extracted from SOFR futures pricing. This adjustment is applied to the short-end anchor rates before spline computation, ensuring that the curve correctly reflects the step-function dynamics of monetary policy.

Remark 3.5. The FOMC meeting schedule is known in advance — the Federal Reserve publishes the calendar for the current and following year. The oracle can therefore pre-load FOMC dates and update the piecewise-constant path estimate whenever futures prices change. Between FOMC meetings, the short-end anchor rates are relatively stable; the oracle's TWAP captures this stability accurately. The primary adjustment occurs in the days surrounding FOMC announcements, when futures prices reprice rapidly and the TWAP must catch up. The 1-hour TWAP at the short end minimizes this lag.

H. Summary of Section 3

The CIRCA rate curve is a natural cubic spline constructed from 15 anchor points in a two-zone density design, stored on-chain as 56 coefficients and evaluable at any tenor in constant time. The following results have been established:

Result 3.1. The spline interpolation error is bounded at 0.052 basis points across the full supported tenor range $[1/12, 30]$ under historically calibrated yield curve parameters — approximately 673 times smaller than the TradFi duration approximation error for off-benchmark tenor targets (Theorem 3.1, Corollary 3.1).

Result 3.2. The maximum profit extractable by manipulating the CIRCA rate curve is bounded by $\Pi_{max} = \text{ADV01}^2/(4c \cdot 0.0001 \cdot D_k \cdot w)$ — quadratic in the attacker's permitted position DV01 and inversely proportional to underlying market depth and TWAP window length. Under the proposed bucket caps and the 24-hour long-end TWAP, the bound at the weakest anchor is approximately \$1,260, roughly two orders of magnitude below the fixed costs of mounting the attack (Theorem 3.2, Remark 3.4, Corollary 3.2).

Result 3.3. Single-anchor manipulation contaminates the interpolated curve only within adjacent tenor intervals, by the locality property of cubic spline basis functions. Full-curve manipulation requires simultaneous attack on all 15 anchors at cost proportional to the sum of all anchor market depths (Theorems 3.3, Corollary 3.3).

Result 3.4. The oracle design incorporates FOMC jump handling at the short end, multi-source aggregation for all anchors, and asymmetric TWAP windowing that minimizes staleness at the short end while maximizing manipulation resistance at the long end.

Together, these results establish that the CIRCA rate curve is both accurate enough to support the continuous tenor parameter of Section 2 and robust enough to resist economically motivated manipulation by any adversary operating within the constraints of the on-chain settlement environment.

IV. The Risk Model

A. Overview

A rate derivatives framework requires a risk model that correctly measures the sensitivity of positions to rate movements, aggregates that sensitivity across a portfolio, and determines the margin required to ensure the solvency of the central counterparty under adverse but plausible market conditions. This section develops the CIRCA risk model in three parts.

Section 4.2 establishes the DV01 framework — the primary measure of rate sensitivity for CIRCA positions. It proves that DV01 aggregation across positions with arbitrary continuous tenors is exact, exploiting the zero-convexity property of the perpetual funding mechanism. Section 4.3 proves the capital efficiency advantage of the unified liquidity pool over fragmented per-tenor alternatives, quantifying the margin reduction achievable through cross-tenor netting under empirically calibrated correlation. Section 4.4 specifies the margin model — initial margin computation, variation margin settlement, and liquidation mechanics — to a level of detail sufficient for implementation, while acknowledging the boundary between the margin model as presented here and a full regulatory-grade margin methodology.

B. The DV01 Framework

1) Single Position DV01: The DV01 of a CIRCA position was established in Theorem 2.2. We restate it here in the context of the risk model and extend it to portfolio aggregation.

Proposition 4.1 *(Single Position DV01)***.** For a CIRCA position $\mathcal{P} = (N, d, K, \tau, t_0, \Delta, \mathcal{O})$, the DV01 at any time $t \geq t_0$ is:

$$\mathrm{DV01}(\mathcal{P}) = N \cdot \tau \cdot 0.0001 \tag{4.1}$$

This quantity is constant in calendar time, independent of the elapsed holding period, and independent of the current oracle rate. It depends only on the notional N and the tenor τ fixed at inception.

Proposition 4.2 *(Zero Convexity)***.** The dollar convexity of a CIRCA position is identically zero:

$$\Gamma(\mathcal{P}) = \frac{\partial^2 V}{\partial \epsilon^2} = 0$$

where ϵ is a parallel basis point shift of the rate curve.

Proof. The position's value has two components (Definition 2.5): the funding stream, with each payment $F_k = N \cdot d \cdot (K - \mathcal{O}(t_{k-1}, \tau)) \cdot \Delta$ linear in the oracle rate, and the mark $M(t) = N \cdot d \cdot (\mathcal{O}(t, \tau) - K) \cdot \tau$, likewise linear in the oracle rate with a constant scale factor τ and no discount factor. A parallel shift of ϵ basis points changes each component at a constant first derivative; the second derivative of each with respect to ϵ is identically zero. Therefore $\Gamma(\mathcal{P}) = 0$. □

Remark 4.1 *(Implications of Zero Convexity)***.** Zero convexity has two important consequences for the risk model. First, DV01 is an exact measure of rate sensitivity — not a first-order approximation — for any magnitude of rate shift. Second, the DV01 aggregation across a portfolio of CIRCA positions is exact for parallel shifts and exact by tenor bucket for non-parallel shifts. There is no convexity adjustment required. This is a significant simplification relative to TradFi IRS risk models, where convexity corrections are mandatory for large portfolios or long-duration positions.

The absence of convexity also has an implication for participants: CIRCA positions cannot be used alone to replicate positively convex instruments such as bonds with embedded options or mortgage-backed securities. This limitation is stated explicitly in Section 6.

2) Portfolio DV01 Aggregation: Consider a pool containing m open CIRCA positions $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ with tenors $\{\tau_1, \tau_2, \ldots, \tau_m\}$, notionals $\{N_1, N_2, \ldots, N_m\}$, and directions $\{d_1, d_2, \ldots, d_m\}$ where $d_i = +1$ for pay-fixed and $d_i = -1$ for receive-fixed.

Theorem 4.1 *(Portfolio DV01 Additivity)***.** The net portfolio DV01 of the pool under a parallel rate shift is:

$$\mathrm{DV01}_{net} = \left| \sum_{i=1}^{m} d_i \cdot N_i \cdot \tau_i \cdot 0.0001 \right| \tag{4.2}$$

This aggregation is exact — not a first-order approximation — for all parallel shifts, by Proposition 4.2.

Proof. Under a parallel shift of ϵ basis points, the change in total pool value is:

$$\Delta V_{pool} = \sum_{i=1}^{m} d_i \cdot N_i \cdot \epsilon \cdot 0.0001 \cdot \Delta \cdot n_i$$

where n_i is the number of remaining funding intervals for position i. For the DV01 computation, we evaluate at the horizon of one basis point over one year: the contribution of position i is $d_i \cdot N_i \cdot \tau_i \cdot 0.0001$, and the net portfolio DV01 is the absolute value of the sum. Since the second derivative is zero by Proposition 4.2, no higher-order terms arise and the expression is exact. □

3) The Bucketed DV01 Framework: For non-parallel rate shifts — steepening, flattening, butterfly moves — the portfolio's sensitivity must be decomposed by tenor. Define the DV01 density of the pool as:

$$\rho(\tau) = \sum_{i=1}^{m} d_i \cdot N_i \cdot \delta(\tau - \tau_i) \cdot 0.0001 \tag{4.3}$$

where $\delta(\cdot)$ is the Dirac delta function, placing each position's DV01 contribution at its exact tenor point. Under a non-parallel rate shift $\Delta r(\tau)$ varying continuously by tenor, the total pool P&L is:

$$\Delta V_{pool} = \int_{1/12}^{30} \rho(\tau) \cdot \Delta r(\tau)\, d\tau \tag{4.4}$$

In practice, the integral is computed by partitioning the tenor space into $K = 14$ buckets corresponding to the intervals between adjacent anchor points, and evaluating:

$$\Delta V_{pool} = \sum_{k=1}^{14} \Delta r_k \cdot \text{BDV01}_k \tag{4.5}$$

where BDV01_k is the signed bucket DV01:

$$\text{BDV01}_k = \sum_{i:\, \tau_i \in [T_k, T_{k+1}]} d_i \cdot N_i \cdot \tau_i \cdot 0.0001 \tag{4.6}$$

The protocol maintains $\{\text{BDV01}_k\}_{k=1}^{14}$ in real time, updated on each position open and close. This 14-element vector is the pool's complete first-order risk representation. Because CIRCA positions have zero convexity, this vector is also the complete risk representation without approximation — no gamma matrix or higher-order terms are required.

The AMM spread function uses the bucket DV01 vector to compute imbalance at any tenor τ. For a position being opened at tenor τ in bucket k:

$$\sigma_{AMM}(\tau) = \sigma_0 + \kappa \cdot \left(\frac{\text{BDV01}_k}{\text{BDV01}_k^{max}} \right)^2 \tag{4.7}$$

where σ_0 is the base spread, κ is the steepness parameter, and BDV01_k^{max} is the governance-set maximum bucket DV01 used to normalize the imbalance ratio. The quadratic form ensures spreads widen slowly when the book is nearly balanced and accelerate as imbalance grows — concentrating the price signal where the pool's risk is highest.

C. *Capital Efficiency of the Unified Pool*

1) Fragmented vs. Unified Pool Architecture: We now prove the capital efficiency advantage of the unified pool. Consider two architectures managing the same aggregate set of CIRCA positions:

Architecture F (Fragmented): $K = 14$ independent pools, one per tenor bucket. Each pool holds capital L_k sufficient to cover its own worst-case net DV01 exposure independently. The total capital requirement is:

$$C_F = \sum_{k=1}^{14} L_k \geq \sum_{k=1}^{14} |\text{BDV01}_k| \cdot \sigma_r \cdot z_\alpha \cdot 10000 \tag{4.8}$$

where σ_r is the annualized rate volatility, z_α is the confidence level multiplier for the chosen coverage probability α, and the factor of 10000 converts DV01 (dollars per basis point) to a dollar P&L for a σ_r-standard-deviation rate move.

Architecture U (Unified): One pool with total capital L sufficient to cover the worst-case portfolio loss across all tenor buckets simultaneously. The loss under a general rate shift $\boldsymbol{\Delta r} = (\Delta r_1, \ldots, \Delta r_{14})$ is:

$$\Delta V_{pool} = \sum_{k=1}^{14} \text{BDV01}_k \cdot \Delta r_k = \mathbf{b}^T \boldsymbol{\Delta r}$$

where $\mathbf{b} = (\text{BDV01}_1, \ldots, \text{BDV01}_{14})^T$ is the bucket DV01 vector. The worst-case loss at the α confidence level, assuming $\boldsymbol{\Delta r} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma})$ with cross-tenor covariance matrix $\boldsymbol{\Sigma}$, is:

$$C_U = z_\alpha \cdot \sqrt{\mathbf{b}^T \boldsymbol{\Sigma} \mathbf{b}} \tag{4.9}$$

2) The Cross-Tenor Correlation Structure: The covariance matrix $\boldsymbol{\Sigma}$ encodes how rate moves at different tenor points co-vary. For SOFR rates, the empirical correlation between rate moves at tenors T_j and T_k is well approximated by an exponential decay model:

$$\rho_{jk} = e^{-\lambda |T_j - T_k|} \tag{4.10}$$

with $\lambda \approx 0.1$ from historical SOFR data. This implies:

- Tenors 1 year apart: $\rho \approx e^{-0.1} \approx 0.905$
- Tenors 5 years apart: $\rho \approx e^{-0.5} \approx 0.607$
- Tenors 10 years apart: $\rho \approx e^{-1.0} \approx 0.368$
- Tenors 20 years apart: $\rho \approx e^{-2.0} \approx 0.135$

Adjacent tenor buckets are highly correlated. Pay-fixed exposure at 4.8 years and receive-fixed exposure at 5.2 years partially offset each other in the unified pool — their opposite-direction DV01s nearly cancel under any rate move that affects both tenors similarly. In the fragmented architecture, these positions would be in different pools and provide zero offset.

3) The Capital Efficiency Ratio: **Theorem 4.2** *(Capital Efficiency of Unified Pool)***.** Let $\mathbf{b}$ denote the bucket DV01 vector and $\mathbf{R}$ the cross-tenor correlation matrix with entries $\rho_{jk} = e^{-\lambda |T_j - T_k|}$. The capital efficiency ratio of the unified pool relative to the fragmented pool is:

$$\eta = \frac{C_U}{C_F} = \frac{\sqrt{\mathbf{b}^T \boldsymbol{\Sigma} \mathbf{b}}}{\sum_k |\text{BDV01}_k| \cdot \sigma_k} \leq 1, \qquad \boldsymbol{\Sigma} = \text{diag}(\boldsymbol{\sigma})\, \mathbf{R}\, \text{diag}(\boldsymbol{\sigma}) \tag{4.11}$$

where $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{14})^T$ is the vector of per-bucket rate volatilities. The unified pool is always at least as capital efficient as the fragmented pool ($\eta \leq 1$), with strict inequality whenever any two buckets have non-zero opposite-direction DV01 and non-zero correlation.

Proof. $C_U = z_\alpha \sqrt{\mathbf{b}^T \boldsymbol{\Sigma} \mathbf{b}}$ where $\Sigma_{jk} = \rho_{jk} \sigma_j \sigma_k$. $C_F = z_\alpha \sum_k |\text{BDV01}_k| \sigma_k$. By the Cauchy-Schwarz inequality applied to the quadratic form:

$$\sqrt{\mathbf{b}^T \boldsymbol{\Sigma} \mathbf{b}} \leq \sqrt{\sum_{j,k} |b_j||b_k| \sigma_j \sigma_k} = \sum_k |b_k| \sigma_k$$

with equality only when $\rho_{jk} = 1$ for all j, k — i.e., all rates are perfectly correlated. Since $\lambda > 0$ in the SOFR correlation model, $\rho_{jk} < 1$ for $j \neq k$, so the inequality is strict for any book with positions in more than one bucket. Therefore $C_U < C_F$ and $\eta < 1$. $\square$

Proposition 4.3 *(Efficiency Under Realistic Conditions)***.** For a book with net exposure in the same direction distributed across K buckets with comparable bucket DV01 magnitudes and average pairwise cross-bucket correlation $\bar{\rho}$, the capital efficiency ratio satisfies:

$$\eta = \sqrt{\frac{1 + (K-1)\bar{\rho}}{K}}$$

With $K = 14$ buckets and $\bar{\rho} \approx 0.70$ implied by equation (4.10) over the CIRCA anchor set, $\eta \approx 0.85$ — approximately a 15% capital saving from cross-bucket diversification alone.

Derivation. For equal-magnitude, same-sign bucket DV01s b with common volatility σ, the quadratic form evaluates to $\mathbf{b}^T\mathbf{\Sigma}\mathbf{b} = b^2\sigma^2\left[K + K(K-1)\bar{\rho}\right]$, while C_F corresponds to $Kb\sigma$; the ratio reduces to the stated expression. □

Two clarifications bound the realistic range. First, a fragmented per-tenor architecture still permits netting *within* each bucket — a pay-fixed and a receive-fixed position at the same tenor offset under either architecture. The unified pool's advantage is specifically *cross*-bucket netting. Second, books containing offsetting net exposures across different buckets — net pay-fixed DV01 at one tenor against net receive-fixed DV01 at a correlated neighboring tenor — achieve savings beyond the same-direction diversification bound, because opposite-sign DV01s at highly correlated tenors cancel inside the unified quadratic form but receive no recognition across fragmented pools. For such books the efficiency gain extends to the 30–40% range. The 15–40% range quoted in Corollary 4.1 spans these two regimes.

Corollary 4.1. The unified CIRCA pool requires 15–40% less capital than fragmented per-tenor pools for books with meaningful cross-tenor diversity, under the empirically calibrated SOFR correlation structure. This range is not a modeling artifact — it is a direct consequence of the well-documented cross-tenor correlation of SOFR rates and the signed additivity of DV01 across positions.

D. The Margin Model

1) Initial Margin: Initial margin (IM) is the collateral a participant must post at position open to cover potential adverse mark-to-market changes over a defined close-out horizon. The CIRCA IM model is inspired by the ISDA Standard Initial Margin Model (SIMM) [11], the industry standard for uncleared derivatives margin, adapted for the perpetual structure and continuous tenor of CIRCA positions.

Definition 4.1 *(Initial Margin Requirement)***.** The initial margin requirement for a CIRCA position $\mathcal{P}$ at inception is:

$$\text{IM}(\mathcal{P}) = \text{DV01}(\mathcal{P}) \cdot z_\alpha \cdot \sigma_r(\tau) \cdot \sqrt{h} \cdot 10{,}000 \qquad (4.12)$$

where $\sigma_r(\tau)$ is the annualized rate volatility at tenor τ in decimal terms (sourced from historical oracle rate data), z_α is the confidence multiplier for coverage probability α (proposed: $\alpha = 99\%$, $z_{99\%} = 2.576$), and h is the margin period of risk (MPOR) in years — the assumed time required to detect a margin breach, issue a margin call, and complete liquidation. The factor $\sqrt{h}$ scales annualized volatility to the close-out horizon under the standard square-root-of-time convention; the factor $10{,}000$ converts the decimal rate move into basis points for application against DV01.

The MPOR is an explicit governance parameter. We propose $h = 5/252$ (five trading days), matching the cleared-CCP standard, on the following reasoning: the protocol's on-chain liquidation pipeline — a 6-hour margin call grace period followed by permissionless keeper execution — is mechanically faster than five days, but the conservative MPOR compensates for the absence of a regulatory backstop and for liquidation-liquidity uncertainty in stressed conditions. Governance may set h more conservatively; it should not set it below the realistic liquidation timeline.

Numerical Example. For a position with $N = \$10\text{M}$, $\tau = 5$ years, $\sigma_r(5Y) = 80$ bps/year, $\alpha = 99\%$, and $h = 5/252$: the position's DV01 is $\$10\text{M} \times 5 \times 0.0001 = \$5{,}000$ per basis point, and the 99th-percentile five-day rate move is $2.576 \times 80 \times \sqrt{5/252} \approx 29.0$ basis points, giving:

$$\text{IM} = \$5{,}000 \times 29.0 \approx \$145{,}000$$

approximately 1.45% of notional — comparable in magnitude to cleared-CCP initial margin for five-year swaps of similar size, and materially below the bilateral uncleared standard, which prescribes a ten-day MPOR. The CIRCA margin model thus prices close-out risk at cleared-market levels while remaining a pure function of on-chain observable quantities.

Portfolio Margin. For a participant holding multiple CIRCA positions, the portfolio IM requirement is computed using the bucket DV01 framework:

$$\text{IM}_{portfolio} = z_\alpha \cdot \sqrt{h} \cdot \sqrt{\mathbf{b}^T\mathbf{\Sigma}\mathbf{b}} \cdot 10{,}000 \qquad (4.13)$$

where $\mathbf{b}$ is the participant's signed bucket DV01 vector and $\mathbf{\Sigma}$ is the cross-tenor covariance matrix. This is the same quadratic form as equation (4.9), applied at the participant level. Portfolio margin is always less than or equal to the sum of individual position margins, with equality only when all positions are perfectly correlated and in the same direction — the worst case for the pool.

2) Variation Margin: Variation margin (VM) reflects the mark-to-market change in position value since the previous VM settlement. For a CIRCA position, the mark-to-market value at time t relative to inception is:

$$\text{MTM}(\mathcal{P}, t) = M(t) = N \cdot d \cdot (\mathcal{O}(t,\tau) - K) \cdot \tau \qquad (4.14)$$

consistent with the position mark of Definition 2.5 — linear in the oracle rate, scaled by the tenor, with no discount factor (see the duration normalization discussion in Section 2.6). The mark is positive for a pay-fixed position when the current oracle rate exceeds the locked fixed rate, and positive for a receive-fixed position when the oracle rate sits below it.

VM Settlement. VM is settled at each funding interval — the same cadence as the funding payment itself. At time t_k, the VM payment is:

$$\mathrm{VM}_k = \mathrm{MTM}(\mathcal{P}, t_k) - \mathrm{MTM}(\mathcal{P}, t_{k-1}) \tag{4.15}$$

If $\mathrm{VM}_k > 0$, the participant's margin account is credited; if $\mathrm{VM}_k < 0$, it is debited. VM payments are settled in the position's denominated currency (typically USDC) from the participant's margin account. The combination of funding payments and VM settlements means that the total daily cash flow to a CIRCA position holder equals the economic gain or loss from rate moves — exactly as in a marked-to-market TradFi IRS.

3) Collateral and Haircuts: Margin may be posted in any asset from the approved collateral set. Each collateral asset carries a haircut $h_a \in [0, 1)$ reflecting its price volatility and liquidation risk — the margin value of one dollar of collateral asset a is $(1 - h_a)$ dollars. The collateral set and haircuts are governance parameters; the proposed initial set is:

Haircut updates are subject to a 48-hour governance time-lock and may not reduce any haircut by more than 5 percentage points per update — preventing governance attacks from artificially inflating collateral values to enable under-margined positions.

4) Margin Call and Liquidation: **Definition 4.2** *(Maintenance Margin)***.** The maintenance margin threshold is:

$$\mathrm{MM} = \gamma \cdot \mathrm{IM}_{portfolio} \tag{4.16}$$

with $\gamma = 0.75$ (proposed). When a participant's margin account balance falls below MM, a margin call is issued.

Liquidation Protocol. If the margin account balance is not restored to $\mathrm{IM}_{portfolio}$ within a grace period of 6 hours following a margin call, any permissionless keeper may trigger liquidation. The liquidation process proceeds as follows:

(i) The pool selects the liquidation priority order — positions are ranked by their contribution to the margin shortfall, with the largest contributors liquidated first

(ii) For each liquidated position, the pool computes the final mark-to-market value and executes a forced close, netting the position's MTM against the participant's collateral

(iii) Collateral is liquidated at oracle price less a liquidation discount $\delta_{liq} = 2\%$, compensating the keeper for execution risk and incentivizing timely liquidation

(iv) Any remaining collateral after satisfying the position's obligations is returned to the participant

(v) If the participant's collateral is insufficient to cover the position's obligations — a shortfall event — the deficit is drawn from the protocol's insurance fund

Definition 4.3 *(Insurance Fund)***.** The insurance fund is a separate reserve pool capitalized by a fraction ϕ of all protocol fee revenue (proposed: $\phi = 20\%$) plus an initial bootstrap capitalization. The fund absorbs shortfall events that exceed a liquidated participant's posted collateral. If the insurance fund is depleted — an event the manipulation resistance analysis of Section 3 suggests would require extraordinary and expensive coordinated attack — a pro-rata loss socialization mechanism is triggered, applying losses to LP positions in proportion to their pool share.

Remark 4.2 *(Comparison to TradFi CCP Recovery)***.** The insurance fund and loss socialization mechanism are the CIRCA equivalents of TradFi CCP recovery and resolution procedures under CPMI-IOSCO guidelines [13]. The key differences are: (i) the CIRCA mechanism is fully encoded in smart contract logic, eliminating discretionary management during stress events; (ii) the loss waterfall is transparent and auditable by any participant before they enter the pool; (iii) there is no regulatory backstop — the fund is the final line of defense. The absence of a regulatory backstop is a genuine limitation stated in Section 6.

E. Summary of Section 4

The CIRCA risk model rests on three results established in this section:

Result 4.1. The DV01 of a CIRCA position is $N \cdot \tau \cdot 0.0001$, exact and constant in time. Portfolio DV01 aggregation across arbitrary continuous tenor positions is exact under parallel shifts and exact by tenor bucket under non-parallel shifts, with no convexity correction required (Propositions 4.1, 4.2; Theorem 4.1).

Result 4.2. A unified liquidity pool with cross-tenor portfolio margining requires 15–40% less capital than fragmented per-tenor pools under the empirically calibrated SOFR cross-tenor correlation structure, with the efficiency advantage derived analytically from the Cauchy-Schwarz inequality and the signed additivity of DV01 (Theorem 4.2, Proposition 4.3, Corollary 4.1).

Result 4.3. The CIRCA margin model — initial margin computed from DV01 and tenor-specific rate volatility, variation margin settled at each funding interval, and a governance-controlled collateral set with time-locked haircut updates — produces IM requirements comparable in magnitude to cleared-CCP standards under a five-day margin period of risk, while incorporating the capital efficiency gains of Result 4.2 for diversified portfolios (Definition 4.1, equation 4.12).

Together, the DV01 framework, the unified pool efficiency proof, and the margin model constitute a complete first-order risk management system for the CIRCA protocol. The system is exact where exactness is achievable (DV01 aggregation), conservative where uncertainty requires it (haircut governance, insurance fund sizing), and honest about its limitations where they exist (no regulatory backstop, no convexity management).

V. Implementation Appendices

A. Overview

The CIRCA framework as developed in Sections 2–4 is platform-agnostic. The financial model — the perpetual funding mechanism, the continuous tenor parameter, the spline rate curve, the DV01 risk framework — is correct regardless of the infrastructure on which it is deployed. Platform choice is an engineering decision that affects performance, cost, liquidity bootstrapping, and sovereignty, but does not alter the mathematical properties proved in the preceding sections.

This section evaluates four deployment targets: EVM-native deployment on a general-purpose Layer 1 or Layer 2

TABLE VI: Proposed Collateral Assets and Haircuts

Asset	Type	Proposed Haircut	Rationale
USDC	USD stablecoin	0%	Dollar-denominated, highly liquid
USDT	USD stablecoin	2%	Minor depegging history warrants small haircut
ETH	Native asset	15%	Price volatility; deep on-chain liquidity
wstETH	Liquid staked ETH	17%	ETH haircut plus staking mechanism risk
OUSG / BUIDL / USTB	Tokenized T-bills	1%	Near risk-free, minor liquidity discount

(Appendix A), deployment on Hyperliquid's HyperCore via the HIP-3 permissionless market framework (Appendix B), deployment on a purpose-built application-specific blockchain (Appendix C), and a hybrid TradFi-DeFi deployment model (Appendix D). Each appendix follows the same structure: what the platform provides natively relevant to CIRCA, what must be built, and an honest assessment of the tradeoffs.

The appendices are not exhaustive — they do not cover every chain or every possible deployment configuration. They are illustrative of the design space, intended to demonstrate that the CIRCA framework is genuinely portable and that the platform choice involves real tradeoffs that cannot be dismissed in either direction.

Appendix A: EVM-Native Deployment

A.1 What EVM Provides: A general-purpose EVM environment — whether Ethereum mainnet, an Ethereum Layer 2 (Arbitrum, Optimism, Base), or an EVM-compatible Layer 1 — provides:

Smart contract programmability. The full CIRCA position lifecycle — open, fund, settle, close, liquidate — can be implemented in Solidity with complete on-chain auditability. Every state transition is deterministic, transparent, and verifiable by any participant.

Composability. EVM composability allows CIRCA positions to interact with the broader DeFi ecosystem without trust assumptions. A CIRCA position's NFT can be used as collateral in a lending protocol, its mark-to-market value can be read by an external contract, and its funding payments can be automatically routed to a yield aggregator — all within a single atomic transaction.

Established security tooling. EVM contracts benefit from a mature ecosystem of formal verification tools, auditing firms, and battle-tested libraries. The security of EVM-deployed financial contracts is better understood empirically than any alternative runtime environment.

Existing liquidity. Layer 2 networks in particular have significant existing liquidity in stablecoins, liquid staked assets, and tokenized RWAs — the assets that serve as CIRCA collateral. LP capital does not need to be bridged from a foreign ecosystem.

A.2 What Must Be Built: EVM deployment requires building the clearing, execution, and oracle infrastructure that more specialized environments provide natively:

The CCP contract. The central counterparty — position registry, margin accounting, portfolio DV01 tracking, liquidation engine, insurance fund — must be implemented from scratch. This is the most complex and security-critical component. The margin model of Section 4 provides the complete specification; the implementation requires careful fixed-point arithmetic and extensive adversarial testing.

The spline oracle. The 15-anchor rate curve, TWAP aggregation, spline coefficient computation, and on-chain evaluation function must be implemented in Solidity using fixed-point arithmetic. The $O(n)$ Thomas algorithm for spline coefficient computation and the $O(\log n)$ binary search for interval identification are both straightforward to implement but must be verified for numerical precision under all valid input ranges.

The AMM. The unified liquidity pool with the DV01-weighted spread function of equation (4.7) requires a custom AMM implementation. No existing EVM AMM design directly supports the bucketed DV01 imbalance model — this is novel infrastructure.

The position NFT. Each CIRCA position is represented as an ERC-721 token with a transfer guard that prevents transfer to addresses with insufficient margin. The override of the ERC-721 transfer function requires careful implementation to prevent the naked transfer attack vector identified in the earlier specification documents.

A.3 Performance Characteristics: EVM performance imposes constraints that affect the CIRCA user experience:

Block time. Ethereum mainnet produces blocks approximately every 12 seconds. Layer 2 networks achieve 0.25–2 second block times. The 8-hour funding interval adopted in Section 2.7 means that funding settlement is not time-sensitive at the block level — the interval is 2,400 Ethereum mainnet blocks, which is adequate for any keeper infrastructure.

Gas cost. The most gas-intensive CIRCA operations are position open (spline evaluation, margin computation, NFT mint, CCP registration) and funding settlement (spline evaluation, DV01 update, payment execution). On Ethereum mainnet at current gas prices, these operations cost approximately \$5–20 per transaction. On Layer 2 networks, costs are 10–100$\times$ lower. Gas cost is not a barrier to institutional use at these levels but would be prohibitive for very small retail positions — consistent with the institutional focus of the CIRCA design.

Throughput. EVM throughput limits the number of position opens per block. At 15 million gas per block and approximately 200,000 gas per position open, Ethereum mainnet supports approximately 75 position opens per block (approximately 6 per second). Layer 2 throughput is significantly higher. For an institutional rate derivatives protocol, this throughput is adequate — LCH SwapClear processes roughly 50,000 new trades per day across all currencies (based on 3.2 million trades cleared in Q1 2025 [5]), which would require approximately 2 position opens per minute on-chain.

A.4 Tradeoff Assessment: **Advantages:** - Maximum composability with the DeFi ecosystem - Most mature security tooling and auditing ecosystem - No token staking requirement or dependency on external protocol governance - Protocol sovereignty — the CIRCA team controls upgrades and governance - Largest existing DeFi liquidity base for collateral assets

Disadvantages: - Highest implementation complexity — all clearing infrastructure must be built - No native order book — the AMM is the only execution mechanism without additional infrastructure - Performance ceiling below specialized environments — not a constraint at institutional volumes, but visible at retail scale - Smart contract risk is entirely the CIRCA protocol's responsibility — no platform-level security backstop

Assessment. EVM-native deployment is the highest-sovereignty option and the most appropriate for a protocol intended as long-term foundational infrastructure. The implementation complexity is real but the CIRCA specification in Sections 2–4 provides sufficient detail to implement correctly. The AMM-only execution model is a genuine constraint — institutional participants accustomed to order book execution may find it unfamiliar — but is mitigated by the oracle-anchored spread design that ensures the AMM always prices near fair value.

Appendix B: Hyperliquid HyperCore via HIP-3

B.1 What HyperCore Provides: Hyperliquid's HyperCore [23] is a purpose-built high-performance trading engine that provides, natively and without additional construction:

Sub-second order finality. HyperBFT consensus achieves approximately 0.2-second average block time with up to 200,000 orders per second throughput. This is three to four orders of magnitude faster than Ethereum mainnet and significantly faster than any current EVM Layer 2.

Native on-chain order book. HyperCore operates a fully on-chain central limit order book (CLOB) — the standard execution mechanism for institutional derivatives markets. Limit orders, market orders, and post-only orders are supported natively. Market makers can quote and cancel at sub-second frequency without gas cost friction.

Native margining and clearing. HyperCore includes a built-in margin engine and risk management system used for all native perpetual markets. HIP-3 deployers inherit access to this infrastructure, reducing the clearing infrastructure that must be custom-built.

HyperEVM composability. Smart contracts deployed on HyperEVM can directly read HyperCore order book state and execute trades within the same consensus layer — eliminating the oracle latency that would otherwise exist between the execution venue and the smart contract layer.

B.2 What Must Be Built on HIP-3: Despite the substantial native infrastructure, a CIRCA deployment on HIP-3 requires significant adaptation:

The rate curve oracle. HyperCore's native oracle is designed for asset price feeds, not for interest rate curves. The 15-anchor spline oracle of Section 3 — including the TWAP aggregation, the piecewise-constant FOMC adjustment, and the spline coefficient computation — must be implemented as a HyperEVM smart contract that feeds rates into the HIP-3 market configuration. The interface between the smart contract oracle and HyperCore's native funding rate mechanism requires custom integration.

Tenor parameterization. HIP-3 markets are configured at deployment time with fixed parameters — a HIP-3 market is a specific perpetual contract, not a generalized framework. Implementing the continuous tenor parameter requires either: (a) deploying a separate HIP-3 market per tenor bucket (fragmenting liquidity), or (b) implementing a HyperEVM smart contract that maps continuous tenor inputs to HyperCore's funding rate mechanism via a custom settlement layer. Option (b) is more consistent with the CIRCA design but requires bespoke integration that the HIP-3 specification does not natively support.

The unified liquidity pool. HyperCore's liquidity model is market-specific — each HIP-3 deployer manages their own liquidity independently. The cross-tenor unified pool of Section 4.3, with its DV01-weighted portfolio margining and correlation-adjusted capital efficiency, has no native equivalent in HyperCore. It must be implemented as a HyperEVM contract that sits above the HyperCore clearing layer.

B.3 The HIP-3 Staking Requirement: HIP-3 deployment on Hyperliquid mainnet requires staking 500,000 HYPE tokens — approximately \$5–10 million at recent prices, though this figure fluctuates with token price. This staking requirement:

- Gates access to the infrastructure behind a capital threshold denominated in a volatile asset
- Creates a dependency on Hyperliquid's token economics and governance — the staking requirement and its terms can be changed by Hyperliquid's governance
- Constitutes a recoverable but illiquid capital commitment for the duration of the deployment
- Is not a reflection of the CIRCA protocol's creditworthiness or soundness, but would be perceived as a cost of operation by institutional evaluators

For a protocol intended as public-good infrastructure, a deployment gate denominated in a third-party token represents a meaningful sovereignty constraint.

B.4 Tradeoff Assessment: **Advantages:** - Dramatically superior execution performance — sub-second finality, 200,000 orders/second - Native CLOB provides institutional-grade order book execution without custom infrastructure - Existing Hyperliquid user base provides liquidity bootstrapping potential - Native margining reduces CCP implementation complexity

Disadvantages: - 500,000 HYPE staking requirement — capital cost, volatility exposure, and sovereign dependency - Continuous tenor parameterization requires bespoke integration not natively supported by HIP-3 - Unified cross-tenor liquidity pool requires custom HyperEVM implementation above HyperCore - Protocol governance is partially subject to Hyperliquid validator and governance decisions - Limited composability with the broader EVM DeFi ecosystem — collateral assets, yield sources, and integrations are Hyperliquid-specific

Assessment. HyperCore via HIP-3 offers the most performant execution environment available for an on-chain derivatives protocol. The CLOB infrastructure and margining system are directly relevant to CIRCA's needs. However, the continuous tenor parameterization — the CIRCA framework's most distinctive contribution — does not map cleanly onto HIP-3's fixed-market architecture without significant custom engineering. The staking requirement and governance dependency are meaningful constraints for a protocol designed as sovereign infrastructure. HIP-3 is best understood as a potential deployment target for a future production implementation once the CIRCA framework is validated, rather than as the natural first deployment environment.

Appendix C: Application-Specific Blockchain

C.1 The App-Chain Model: An application-specific blockchain — a sovereign chain built using the Cosmos SDK, Polkadot parachain framework, or a custom consensus design — provides maximum flexibility at the cost of bootstrapping an independent validator set and cross-chain interoperability infrastructure.

C.2 What an App-Chain Provides: **Custom consensus parameters.** Block time, finality model, and throughput can be designed specifically for rate derivatives — for example, a 1-second block time with deterministic finality, eliminating the probabilistic finality risk that affects Ethereum mainnet.

Native financial primitives. The chain's state machine can encode CIRCA-specific logic at the protocol level — position accounting, margin computation, and funding settlement can be implemented as native module functions rather than EVM bytecode, achieving significant performance and gas cost advantages.

No shared blockspace contention. A dedicated chain eliminates the gas price volatility that affects EVM deployment during market stress events — precisely when CIRCA operations (margin calls, liquidations) are most time-sensitive.

Full governance sovereignty. All protocol parameters — oracle sources, haircuts, funding intervals, position size limits — are governed by the chain's native governance mechanism without dependency on any external protocol.

C.3 What Must Be Built: An app-chain deployment requires building essentially everything:

Validator infrastructure. A new chain requires a validator set willing to run the chain's nodes. Bootstrapping a credible, decentralized validator set is a multi-year effort requiring significant coordination and economic incentives.

Cross-chain bridges. Collateral assets (USDC, wstETH, tokenized T-bills) live on Ethereum and other chains. Bringing them to an app-chain requires bridge infrastructure, introducing the bridge security risks that are among the most significant attack vectors in the current DeFi ecosystem.

Block explorer, tooling, and developer ecosystem. The full infrastructure stack expected by institutional participants — block explorers, API providers, wallet integrations, auditing tooling — must be built or adapted for the new chain.

C.4 Tradeoff Assessment: **Advantages:** - Maximum performance and customizability - Full governance sovereignty - No shared blockspace contention - Native financial primitives possible

Disadvantages: - Highest bootstrapping cost and complexity — years of infrastructure development before deployment - Bridge risk for collateral assets — currently one of the most significant attack vectors in DeFi - Validator set bootstrapping requires significant coordination and economic commitment - Isolation from DeFi ecosystem composability

Assessment. The app-chain model represents the long-term architectural endpoint for a CIRCA deployment at institutional scale — analogous to how dYdX v4 migrated from EVM to a Cosmos app-chain as volumes grew [24]. It is not appropriate as a first deployment target given the bootstrapping requirements. A credible path would be: EVM-native deployment for initial validation, HIP-3 deployment for performance scaling, and app-chain migration if and when volumes justify the infrastructure investment.

Appendix D: TradFi Hybrid Deployment

D.1 The Hybrid Model: A fourth deployment model — not yet implemented anywhere in the DeFi ecosystem — would layer the CIRCA framework onto existing TradFi clearing infrastructure. In this model, the rate curve, position NFTs, and funding calculations live on-chain, while margin posting and settlement occur through established channels: DTCC, Fedwire, or a prime brokerage relationship.

D.2 Rationale: The hybrid model directly addresses the legal enforceability and regulatory capital treatment limitations identified in Section 6. If CIRCA positions are cleared through a recognized CCP — LCH or CME — the regulatory capital treatment for bank participants is the same as for TradFi IRS. The on-chain components provide transparency and auditability; the TradFi clearing components provide legal enforceability and regulatory recognition.

D.3 Requirements and Obstacles: Implementing the hybrid model requires:

Legal mapping. A legal opinion mapping the on-chain CIRCA position definition to an ISDA-recognized swap confirmation. Several law firms have begun this work for other on-chain derivatives protocols; the CIRCA framework's formal mathematical definition simplifies this mapping relative to less precisely specified protocols.

CCP recognition of on-chain positions. LCH and CME would need to recognize CIRCA smart contract positions as eligible for clearing — a regulatory and commercial decision that neither organization has made for any on-chain protocol to date.

Oracle integration with TradFi data. The CIRCA rate curve uses on-chain oracle rates. A hybrid deployment would need to reconcile these rates with TradFi reference rates in a legally recognized way — potentially substituting CME Term SOFR for the on-chain SOFR futures-derived anchor rates at the short end.

D.4 Assessment: The hybrid model is the most ambitious and most impactful deployment path — it is the version of CIRCA that could attract regulated bank treasuries, insurance companies, and pension funds as direct participants. It is also the most distant from current feasibility. The regulatory and legal infrastructure required does not yet exist, and building it requires engagement with regulators, clearinghouses, and legal counsel across multiple jurisdictions. The CIRCA framework's mathematical precision is a prerequisite for this path — a protocol that cannot be formally specified cannot be legally mapped to ISDA documentation — but mathematical precision alone is not sufficient. This path is included here to mark the direction of travel rather than to present a near-term implementation option.

B. Implementation Comparison Summary

No deployment target dominates across all dimensions. The appropriate choice depends on the implementer's priorities — sovereignty versus performance, near-term feasibility versus long-term institutional reach, DeFi composability versus regulatory recognition. The CIRCA framework is designed to remain correct and valuable regardless of which path is taken.

VI. Open Problems and Limitations

A. Overview

The preceding sections establish that the CIRCA framework provides a mathematically rigorous and provably superior structure for on-chain interest rate swaps along specific dimensions: continuous tenor parameterization, persistent duration, capital efficiency from cross-tenor netting, and manipulation-resistant rate curve construction. This section enumerates the limitations of the framework and the open problems that remain unsolved. Some of these limitations are amenable to future extension of the framework; others represent fundamental boundaries imposed by the structural choices made in Sections 2–4. Distinguishing between these two categories is the purpose of this section.

The limitations are organized into four groups: structural properties of the perpetual instrument (Section 6.2), infrastructure and oracle constraints (Section 6.3), legal and regulatory gaps (Section 6.4), and empirical and methodological caveats (Section 6.5). Section 6.6 identifies extensions to the framework that could address some of these limitations and outlines the research required.

B. Structural Limitations of the Perpetual Instrument

1) Zero Convexity: Proposition 4.2 established that CIRCA positions have zero dollar convexity. This is a structural consequence of the funding payment's linearity in the oracle rate, and it is the source of the framework's risk model simplicity — DV01 aggregation is exact rather than first-order.

Zero convexity is also a limitation. Several important categories of TradFi instruments exhibit positive convexity that participants actively seek to manage:

- **Long-duration bonds** held to maturity have positive convexity from the discount factor — their value declines less than DV01 alone would predict for large rate increases, providing partial protection against rate shocks
- **Bonds with embedded options** — callable corporates, putable Treasuries — carry option-like convexity
- **Mortgage-backed securities** exhibit negative convexity from prepayment optionality, requiring active convexity hedging that is itself a significant component of the rates market

A participant whose hedging mandate involves managing convexity exposure — for example, a mortgage REIT hedging the convexity profile of its agency MBS portfolio — cannot achieve their objective using CIRCA positions alone. The CIRCA framework is appropriate for linear duration exposure; it is not a replacement for the full TradFi rates toolkit.

Implication. Participants requiring convexity management must either combine CIRCA positions with other instruments (on-chain options on the rate curve, if and when such instruments exist) or continue to use TradFi infrastructure for the convexity component of their exposure. The CIRCA framework does not preclude the development of complementary on-chain convexity instruments, but designing them is beyond the scope of this paper.

2) Persistent Duration as a Two-Sided Property: Theorem 2.2 established that CIRCA positions have constant DV01 in time — the persistent duration property. This was presented as a feature relative to TradFi IRS, eliminating roll costs and operational complexity for participants seeking persistent rate exposure.

The same property is a limitation for a different class of participants. Some hedging mandates require duration that declines as a known liability approaches — a pension fund's expected benefit payments, a corporate bond issuer's known refinancing date, a structured product's scheduled cash flow profile. For these participants, the natural duration decay of a fixed-maturity IRS is not a bug to be eliminated but a desirable structural property that aligns the hedge with the underlying exposure.

A participant managing a declining duration mandate using CIRCA positions must actively close and reopen positions to reduce notional over time, incurring transaction costs and timing risk that fixed-maturity IRS avoid by construction. The framework does not prevent this — partial close functionality is supported — but it does not provide automatic decay either.

Implication. CIRCA is optimized for persistent duration exposure. Participants with mandates that align naturally with fixed-maturity decay may find TradFi IRS structurally better suited. A future extension of the framework could introduce a maturity parameter that converts the perpetual to a fixed-maturity equivalent, but this would forgo the persistent duration advantage and is therefore left as a deliberate design boundary rather than a planned extension.

3) The Tenor Reference Interpretation: Section 2.5 established that a CIRCA position is economically equivalent to a continuously-rolled fixed-maturity IRS, not to a single fixed-maturity instrument. This distinction is mathematically precise but has subtle implications for participants whose hedging mandate is defined relative to a single specific TradFi instrument.

A bank treasurer hedging a 5-year SOFR swap booked in TradFi using a CIRCA 5-year position is not hedging the identical instrument — they are hedging a continuously-rolled equivalent. Under specific scenarios — particularly large discrete moves in the long end of the curve immediately before TradFi roll dates — the CIRCA and TradFi positions will diverge in P&L. The divergence is bounded by the

TABLE VII: Deployment Target Comparison

Dimension	EVM-Native	HyperCore / HIP-3	App-Chain	TradFi Hybrid
Execution performance	Moderate	Excellent	Excellent	TradFi standard
Implementation complexity	High	Moderate–High	Very High	Very High
Continuous tenor support	Native	Requires custom integration	Native	Native
Unified pool architecture	Native	Requires custom integration	Native	Partial
Sovereignty	Full	Partial	Full	Partial
Composability with DeFi	Excellent	Limited	Limited	None
Legal enforceability	Smart contract only	Smart contract only	Smart contract only	Full (if CCP-cleared)
Regulatory capital treatment	Unrecognized	Unrecognized	Unrecognized	Potentially recognized
Bootstrapping cost	Moderate	Moderate + HYPE stake	Very High	Very High
Near-term feasibility	High	Moderate	Low	Very Low

discretization and compounding error analyses of Sections 2.7 and 2.8, but it is non-zero.

Implication. Participants seeking to hedge specific TradFi IRS positions one-for-one cannot achieve perfect replication using CIRCA. The hedge is effective for the rate exposure but not identical at the instrument level. This is acceptable for most economic hedging mandates but may not satisfy accounting hedge effectiveness requirements under IFRS 9 [17] or US GAAP ASC 815 [18], which require strict replication for hedge accounting treatment.

C. Infrastructure and Oracle Limitations

1) Long-End Curve Reliability: Section 3.6 demonstrated that the manipulation resistance of the rate curve is bounded by the market depth of the underlying instruments at each anchor point, with the 30-year anchor representing the binding constraint at approximately $3.3 billion per basis point of market depth. While this depth is sufficient to deter manipulation by all but the most extraordinarily capitalized adversaries, it is also several orders of magnitude thinner than the short-end anchor points.

This asymmetry has two implications. First, the long-end anchors are more sensitive to legitimate market events — a large institutional trade in 30-year SOFR swaps can move the published rate by several basis points, which is signal rather than noise but introduces volatility into the long end of the CIRCA curve that does not affect the short end. Second, in stressed market conditions where 30-year liquidity contracts further — as occurred briefly during the March 2020 Treasury market disruption — the long-end manipulation resistance bound deteriorates, potentially creating windows during which the manipulation-profit bound deteriorates and the per-bucket position caps must carry more of the defensive burden.

Implication. The CIRCA framework's manipulation resistance is strongest at the short end and weakens monotonically as tenor extends. Position size limits at the long end should be set conservatively, and the protocol may need to widen the AMM spread or temporarily restrict new long-tenor position opens during stressed market conditions where 30-year liquidity is impaired. Mechanisms for detecting such conditions and triggering protective responses are not specified in this paper and represent a meaningful infrastructure gap.

2) Oracle Source Concentration: Section 3.5 specified that each anchor rate is aggregated from at least three independent data sources, providing protection against single-source manipulation. This protection is genuine but partial. All three sources for any given anchor are downstream of the same underlying instruments — SOFR futures for the short end, SOFR swap rates for the long end. A coordinated attack on the underlying instruments themselves would propagate to all three sources simultaneously.

The independence between sources protects against single-source operational failures (a data provider going offline, a feed publishing erroneous values) but does not protect against attacks on the underlying market. This limitation is shared by all financial data infrastructure — even TradFi reference rates derive from the same underlying instruments — but it is worth stating explicitly because the "multi-source aggregation" language can suggest a stronger guarantee than is actually provided.

Implication. The manipulation resistance bounds of Section 3 assume an adversary attacking the underlying instruments. They are not weakened by multi-source aggregation, but they are not strengthened by it either. Multi-source aggregation protects against a different and more common class of failures — operational rather than economic — and should be understood as defense in depth rather than as additional manipulation resistance.

3) Cross-Chain Rate Consistency: If the CIRCA framework is deployed on multiple chains — for example, on Ethereum mainnet, Arbitrum, and Base simultaneously — each deployment maintains its own rate curve. The rate curves should converge to the same fair value because they are anchored to the same underlying instruments, but they may diverge transiently during periods of differential oracle update latency or cross-chain bridge stress.

For participants using CIRCA positions on multiple chains to hedge consolidated exposure, transient divergence between the chains' rate curves creates tracking error that has no economic source — it arises purely from oracle update timing differences. The CIRCA framework does not currently specify a mechanism for cross-chain rate consistency.

Implication. Multi-chain deployment introduces a coordination problem that single-chain deployment avoids. The natural solution — a canonical rate curve published on one chain and bridged to others — reintroduces bridge risk into the rate infrastructure. The optimal architecture for multi-chain deployment is an open problem that depends on future developments in cross-chain communication infrastructure.

D. Legal and Regulatory Limitations

1) ISDA Enforceability: A CIRCA position is enforceable as a smart contract: its terms are deterministic, its state is auditable, and its settlement is executed by code that cannot be repudiated. This is enforceability in the technical sense — the contract executes as written.

It is not enforceability in the legal sense recognized by most jurisdictions. The International Swaps and Derivatives Association (ISDA) Master Agreement is the standard legal framework for over-the-counter derivatives globally, and an ISDA-documented swap carries specific legal recognition: it qualifies for netting under bankruptcy law, it is recognized as a financial contract under regulatory frameworks, and disputes are subject to defined legal jurisdiction. A CIRCA position carries none of these properties by default.

The absence of ISDA documentation is not a technical defect of the protocol — it is a categorical gap between smart contract execution and legal enforceability. Closing this gap requires either:

(i) **Legal mapping** — a legal opinion mapping CIRCA positions to ISDA-equivalent confirmations, executed by participating counterparties as part of the position-opening flow. This work is partially underway in adjacent on-chain derivatives projects, but the CIRCA framework does not provide it directly.

(ii) **Regulatory recognition of smart contract derivatives** — explicit acknowledgment by relevant regulators that smart contract derivatives are valid financial contracts. This recognition does not currently exist in any major jurisdiction.

Implication. Participants for whom legal enforceability is a binding constraint — regulated banks, insurance companies, pension funds — cannot use CIRCA positions for their core derivatives activities without parallel ISDA documentation. The framework is well-suited for participants without this constraint (crypto-native institutions, DeFi protocols, family offices with explicit digital asset mandates) but is not a near-term substitute for ISDA-documented IRS in regulated institutional contexts.

2) Regulatory Capital Treatment: Under the Basel III framework [12], the regulatory capital a bank must hold against a derivatives position depends critically on whether the position is cleared through a qualifying CCP. The CIRCA central counterparty, as specified in Section 4, is a smart contract — not a qualifying CCP under any current regulatory framework. A bank holding a CIRCA position must therefore treat it as an uncleared derivative for capital purposes, which carries substantially higher capital charges than the equivalent cleared position.

The capital impact is material. Under the Standardized Approach for Counterparty Credit Risk (SA-CCR), an uncleared SOFR swap with \$10M notional and 5-year tenor generates a counterparty exposure of approximately \$200,000 — corresponding to a Tier 1 capital requirement of approximately \$16,000 at 8% capital ratios. The same position cleared at LCH SwapClear generates a counterparty exposure approximately $5\times$ smaller. For a bank operating at capital efficiency margins, this differential makes uncleared positions economically unattractive even when they are otherwise superior.

Implication. Bank participation in CIRCA at meaningful scale requires either: (i) the protocol's CCP achieving qualifying CCP status, which requires regulatory engagement and operational scrutiny that no on-chain CCP has yet achieved, or (ii) a hybrid deployment that clears through an existing qualifying CCP (the Appendix D model). Neither is near-term feasible. Until one is, regulated bank treasuries will find the regulatory capital treatment of CIRCA positions sufficient to prefer TradFi alternatives.

3) Permissionless Access vs. Compliance Requirements: The CIRCA framework as specified is permissionless: any address can open a position subject to margin requirements. This is consistent with the design philosophy of DeFi infrastructure and provides genuine accessibility benefits — participants without banking relationships, geographic restrictions, or institutional minimums can interact with the protocol on equal terms with the largest participants.

It is not consistent with the regulatory requirements that govern institutional derivatives activity. The Know Your Customer (KYC) and Anti-Money Laundering (AML) frameworks under Dodd-Frank [14] in the US, MiFID II [15] in Europe, and equivalent regulations globally require regulated participants to identify their counterparties. A bank or insurance company entering a derivatives position with an anonymous counterparty is in violation of its regulatory obligations regardless of the position's economic terms.

Implication. Regulated institutional participation requires a permissioned access layer that screens counterparties for KYC/AML compliance. This access layer can sit above the permissionless protocol — institutional participants interact through a compliance-gated frontend that maintains a whitelist — but its existence creates a tension with the protocol's permissionless ethos. The framework supports permissioned access as a deployment option without requiring it at the protocol level. Different deployments may choose different access models depending on their target participant base.

4) Trade Reporting: EMIR [16] in Europe and Dodd-Frank [14] in the US require derivatives trades to be reported to authorized trade repositories. The on-chain record of CIRCA positions provides far more detail than current trade reporting infrastructure captures, but it is not in the format or transmitted through the channels that current regulatory frameworks recognize. Regulated participants using CIRCA must implement parallel reporting infrastructure to satisfy their regulatory obligations.

Implication. This is an operational rather than fundamental limitation — the technology to generate compliant reports from on-chain data exists and is being developed by multiple service providers — but it does represent additional operational cost for regulated participants. The framework does not provide this infrastructure directly.

E. Empirical and Methodological Caveats

1) SOFR History Length: The empirical analysis of Section 2.7 was conducted on the full published history of SOFR from April 2018 to April 2026 — approximately 8 years and 2,013 published business days. This period covers one Federal Reserve hiking cycle (March 2022 – July 2023), one near-zero rate regime (April 2018 – February 2022), and the subsequent plateau. It is sufficient to bound the discretization error under conditions representative of the published SOFR history.

It is not sufficient to bound behavior under regimes that have not yet occurred. A sustained deflationary period with negative policy rates — as observed in some European jurisdictions during 2014–2022 — would produce rate dynamics outside the SOFR sample. A hyperinflationary regime would similarly fall outside the sample. The empirical bounds of Section 2.7 should be understood as calibrated to historical conditions rather than as guarantees under all possible future rate environments.

Implication. The funding interval recommendation of 8 hours is robust within the historical sample. Extension to unsampled rate regimes requires either additional empirical validation as new data becomes available or analytical bounds derived from rate dynamics models calibrated to those regimes. Neither is provided in this paper.

2) Nelson-Siegel Parameter Calibration: The spline interpolation error bound of Theorem 3.1 assumed yield curves consistent with the Nelson-Siegel family of term structure models with parameter bounds calibrated to historically observed values. This is conservative for typical curve shapes but is not a guarantee against pathological curve configurations that fall outside the Nelson-Siegel family.

Specifically, yield curves exhibiting multiple inflection points (a humped curve at the short end combined with a separate hump at the long end), or curves with extreme curvature concentrated at a single tenor, could produce fourth-derivative magnitudes exceeding the bound used in the proof. Such curve shapes are rare empirically but not impossible.

Implication. The 0.052 basis point error bound is robust under typical yield curve dynamics. Under pathological curve shapes, the actual interpolation error could be higher, though it would remain bounded by the geometric term of the spline error formula. The framework's accuracy under stressed curve conditions deserves dedicated empirical validation that this paper does not provide.

3) Cross-Tenor Correlation Stability: The capital efficiency analysis of Section 4.3 assumed cross-tenor correlation following the exponential decay model $\rho_{jk} = e^{-\lambda|T_j - T_k|}$ with $\lambda \approx 0.1$. This is the historically observed correlation structure for SOFR rates over the post-2018 period.

Cross-tenor correlation is not a structural constant. It varies with monetary policy regime, market conditions, and the term structure model implicit in market participants' expectations. During the 2008 financial crisis, cross-tenor correlation in USD swap rates spiked toward 1.0 as all rates moved together in response to systemic risk. During quantitative easing periods, the long end became partially decoupled from the short end as central bank purchases affected long-dated yields independently of policy rate expectations.

Implication. The 15–40% capital efficiency advantage of the unified pool is calibrated to historically observed correlation. Under different correlation regimes, the efficiency advantage could be larger (if correlation drops, allowing more netting benefit) or smaller (if correlation rises toward 1, eliminating the netting benefit). The framework's capital efficiency is therefore regime-dependent, and the proposed margin model should be periodically recalibrated to reflect observed correlation dynamics.

F. Extensions and Research Directions

The limitations identified in Sections 6.2 through 6.5 vary in their tractability. Some represent fundamental boundaries of the perpetual instrument and cannot be addressed without departing from the framework's structural choices. Others represent gaps that future work could close. This section identifies four extensions that appear tractable and would meaningfully expand the framework's applicability.

1) Cross-Currency CIRCA: The framework as developed assumes all positions are denominated in a single currency, with the rate curve referencing SOFR-equivalent rates and collateral posted in a USD stablecoin. A cross-currency extension would support positions where the fixed leg is denominated in one currency and the floating leg in another — for example, a swap exchanging fixed USD payments for floating EUR payments based on €STR.

The mathematical extension is straightforward — the funding payment becomes a difference between two currency-specific rate curves multiplied by an exchange rate — but the practical implementation introduces FX rate dependency, additional oracle complexity, and a new manipulation surface. A formal specification of cross-currency CIRCA, including the cross-currency basis swap component that exists in TradFi markets, is left as an open extension.

2) Amortizing Notional with RWA-Linked Oracles: The framework supports amortizing notional as a deterministic schedule fixed at position open. For positions hedging real-world asset cash flows — mortgage pools, trade receivables, private credit — the actual amortization schedule depends on prepayments and defaults in the underlying pool and is not known in advance.

An RWA-linked amortizing CIRCA position would receive its notional schedule from a trusted oracle reporting the actual amortization of the reference pool. This requires: (i) a recognized RWA tokenization standard with reliable amortization reporting, (ii) an oracle mechanism for ingesting RWA cash flow data on-chain, and (iii) margin model adaptations to handle stochastic notional schedules. The first is partially available through existing RWA protocols; the second and third are open research problems.

3) Convexity Instruments: Section 6.2.1 identified zero convexity as a structural limitation of the perpetual instrument. An extension to the framework could introduce a separate class of instruments — rate options or convexity certificates — that provide explicit convexity exposure for participants who need it. The pricing of such instruments requires a volatility surface for the rate curve, which is itself an open infrastructure problem.

4) Fixed-Maturity Variant: For participants whose hedging mandate naturally aligns with fixed-maturity decay (Section 6.2.2), an alternative instrument with a maturity parameter could supplement the perpetual base offering. This would forgo the persistent duration property of CIRCA but would provide an instrument better matched to a common class of hedging needs. The mathematical extension is direct — the fixed-maturity variant is essentially the TradFi IRS expressed in CIRCA's on-chain infrastructure — but it represents a deliberate framework choice between persistent duration (CIRCA's core innovation) and fixed-maturity flexibility (TradFi's standard).

G. Closing Remarks

The CIRCA framework as presented in this paper is not a complete solution to all problems in on-chain rate derivatives. It is a specification for a particular instrument — a perpetual interest rate swap with continuous tenor parameterization — implemented on a particular infrastructure stack — an on-chain rate curve with cross-tenor netting — and it improves on the TradFi equivalent along specific, provable dimensions. It does not solve the legal enforceability problem. It does not solve the regulatory capital problem. It does not provide convexity instruments or cross-currency exposure or fixed-maturity flexibility. It does not eliminate the structural risks of on-chain financial infrastructure — oracle failure, smart contract vulnerability, liquidity pool concentration.

What it does is establish that the on-chain interest rate swap is not simply a re-implementation of TradFi infrastructure in a new medium. Done correctly, the on-chain version can be a structurally different instrument with structurally different properties — one that exploits the programmable settlement and continuous parameterization properties of the underlying infrastructure to provide capabilities that TradFi cannot. The continuous tenor parameter and the persistent duration property are not incremental improvements on the TradFi IRS. They are new financial capabilities that did not previously exist.

The market for interest rate risk management is ˜$539 trillion in notional and serves the most fundamental financial function of any derivative category. The case for moving even a small fraction of this market on-chain rests on the existence of genuine, quantifiable advantages over the TradFi alternative. This paper has attempted to establish that such advantages exist, to characterize them precisely, and to acknowledge honestly where they do not. The framework is offered as a contribution to the design of financial infrastructure that future markets may adopt — not as a finished product but as a specification rigorous enough to be built upon, examined, criticized, and extended.

References

[1] Bank for International Settlements, "OTC derivatives statistics at end-June 2025," Dec. 2025.
[2] International Swaps and Derivatives Association, "Key Trends in the Size and Composition of OTC Derivatives Markets in the First Half of 2025," Jan. 2026.
[3] Federal Reserve Bank of New York, Secured Overnight Financing Rate (SOFR), retrieved via Federal Reserve Bank of St. Louis, FRED Economic Data.
[4] LCH Group, "SwapClear Volumes," lch.com, 2025.
[5] LCH Group, "SwapClear Q1 2025 Highlights," LSEG, 2025.
[6] DefiLlama, "Pendle: Total Value Locked," defillama.com/protocol/pendle.
[7] A. Afonso, M. Cipriani, A. Copeland, A. Kovner, G. La Spada, and A. Martin, "The Market Events of Mid-September 2019," *Federal Reserve Bank of New York Economic Policy Review*, vol. 27, no. 2, Aug. 2021.
[8] Financial Stability Board, "Holistic Review of the March Market Turmoil," Nov. 17, 2020.
[9] C. R. Nelson and A. F. Siegel, "Parsimonious Modeling of Yield Curves," *The Journal of Business*, vol. 60, no. 4, pp. 473–489, Oct. 1987.
[10] F. X. Diebold and C. Li, "Forecasting the Term Structure of Government Bond Yields," *Journal of Econometrics*, vol. 130, no. 2, pp. 337–364, 2006.
[11] International Swaps and Derivatives Association, "ISDA SIMM Methodology," current version, isda.org.
[12] Basel Committee on Banking Supervision, "The Standardised Approach for Measuring Counterparty Credit Risk Exposures," BCBS 279, Bank for International Settlements, Mar. 2014 (rev. Apr. 2014).
[13] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, "Principles for Financial Market Infrastructures," Apr. 2012.
[14] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 2010.
[15] Markets in Financial Instruments Directive II (MiFID II), Directive 2014/65/EU, European Union.
[16] European Market Infrastructure Regulation (EMIR), Regulation (EU) No. 648/2012, European Union.
[17] International Accounting Standards Board, IFRS 9 *Financial Instruments*.
[18] Financial Accounting Standards Board, ASC 815 *Derivatives and Hedging*.
[19] Pendle Finance, official documentation, docs.pendle.finance.
[20] Notional Finance, official documentation, docs.notional.finance.
[21] Yield Protocol, official documentation, docs.yieldprotocol.com.
[22] Swivel Finance (docs.swivel.finance), Element Finance, and Sense Finance, official protocol documentation. Element Finance and Sense Finance have since discontinued active development.
[23] Hyperliquid, "HIP-3: Permissionless Listing Framework," hyperliquid.gitbook.io.
[24] dYdX Trading Inc., "dYdX v4 (dYdX Chain)," github.com/dydxprotocol/v4-chain.