DECENTRALISED FINANCE · VOL. 1 · APRIL 2026

The Self-Custody Option

Why every options market requires you to give up your assets — and why none of them have to. An argument for escrow-settled, oracle-free, bilateral derivatives.

AUTHOR	RESEARCH	VERSION	IMPLEMENTATION
Shane Calder	April 2026	1.0 — Initial	caput.dev

0	2	0	0
OPTIONS WITH SELF-CUSTODY	WALLETS PER CONTRACT	ORACLES REQUIRED	ASSETS BORROWED

§0

The Core Finding

Every options market ever built — exchange-traded, OTC, DeFi — requires one party to give up custody of their assets for the duration of the contract. A clearinghouse holds them. A smart contract holds them. A protocol treasury holds them. A counterparty desk holds them. The assumption is so embedded it is not questioned. It is just what options require.

It is not what options require. It is what options have always done.

The distinction matters because the custody assumption is the source of every structural risk in derivatives — counterparty failure, exchange insolvency, protocol exploit, admin key compromise. These are not bugs in specific implementations. They are consequences of a design assumption that has persisted for as long as derivatives have existed. Remove the custody assumption and those risks disappear. Not reduced. **Removed.**

THE FINDING

The gap between "non-custodial" and "self-custody" is not a matter of degree. Non-custodial means a smart contract holds your assets instead of a person. Self-custody means nobody holds your assets. The escrow holds them. Your wallet is the only key. That is a different kind of statement about who controls the money.

§1

The Custody Assumption

Three models exist for options today. All three require custody transfer. The intermediary varies — exchange, escrow agent, smart contract — but the pattern is identical. Funds leave the user's control and return only when the intermediary permits.

A · CENTRALISED EXCHANGE	B · OTC DESK	C · DEFI PROTOCOL

User deposits funds. Exchange holds custody. Exchange is counterparty, clearinghouse, and settlement layer. User's assets are pooled. Withdrawal requires permission.	Two parties negotiate. A third party settles. Legal agreements, escrow agents, margin accounts held by intermediaries. Works for eight-figure desks. For everyone else, the overhead eats any premium worth collecting.	User deposits into a smart contract. Protocol holds custody. Oracle feeds price. Settlement is computed against the oracle, not executed against a real market. There is no writer on the other side.
▫ CUSTODY TRANSFERRED ▫ VENUE IS COUNTERPARTY	▫ OVERHEAD PER CONTRACT ▫ SCALES POORLY DOWN	▫ ORACLE DEPENDENCY ▫ POOL IS COUNTERPARTY

D · SELF-CUSTODY OPTION

Two wallets. Three escrows. One multisig with its master key disabled. Funds sit in on-chain escrows for the term. Released only by cryptographic condition. Settlement is a real swap through the AMM. No intermediary holds assets at any point. Both parties sign every transaction in their own wallet. The bot coordinates. It never signs.

▫ SELF-CUSTODY · ▫ NO ORACLE · ▫ BILATERAL · ▫ REAL SETTLEMENT

§2

The Missing Instrument

On most chains and in most markets, derivatives are built on top of borrowing infrastructure. To short an asset you borrow it. To write an option you post margin in a lending pool. To create leveraged exposure you use a margin facility. The entire architecture assumes that somewhere, someone is lending.

On XRPL, that infrastructure does not exist. There is no lending protocol for XRP or RLUSD. There is no margin facility. There are no perpetuals. There is an AMM for spot trading, and that is it. If you want directional exposure to XRP/RLUSD beyond buying and holding spot — in either direction — there is **no on-chain instrument available.**

> *The assumption is that derivatives require borrowing. They do not. They require two parties willing to take opposite sides of a price movement, and a mechanism to settle the outcome. Everything else is infrastructure that existing markets added because they had no other way to enforce the contract.*

The self-custody option requires nothing borrowed and nothing lent. The seller provides the notional. The buyer provides margin and premium. The AMM provides the rate. The escrow provides custody. The instrument is self-contained.

REQUIREMENT	TRADITIONAL DERIVATIVE	SELF-CUSTODY OPTION
Borrowing	Yes — margin lending, short selling	No — seller provides notional directly

Liquidity pool	Yes — protocol or exchange-managed	No — AMM is venue, not counterparty
Oracle	Yes — external price feed	No — AMM rate is the settlement
Custody transfer	Yes — to exchange, protocol, or agent	No — ledger escrow, user wallets only
Intermediary	Yes — clearinghouse, protocol, or desk	No — 2-of-2 multisig, master disabled
Fractional reserve	Yes — leverage through lending	No — fully collateralised by both parties

THE OBSERVATION

This instrument does not exist because the assumption has always been that creating it requires infrastructure that does not exist on XRPL — lending, margin, oracles, protocol governance. The assumption was wrong. The ledger's native primitives — escrow, multisig, AMM — are sufficient. The instrument was always possible. Nobody built it.

§3

The Oracle Assumption

Options need a price to settle against. Every existing implementation solves this with an oracle — an external price feed that tells the contract what the asset is worth at expiry.

The oracle is a dependency. It can be manipulated. It can be stale. It can disagree with the market. It introduces a single point of failure into a system that claims to be decentralised. Hundreds of millions of dollars have been lost to oracle manipulation in DeFi. The problem is not bad oracles. The problem is needing one at all.

ORACLE-SETTLED	AMM-SETTLED
An external system reports that the price is X. The contract computes a payoff against X. The assets never interact with the market. Settlement is a calculation. Whether X is correct is an open question at every expiry.	The locked asset swaps back through the AMM. The swap produces whatever the market gives. Settlement is a trade. There is no X to report, no feed to trust, no oracle to manipulate. The price is the outcome, not an input.

> *An option that settles through a real swap does not need to know the price. The price is whatever the market gives. The AMM is not an oracle. It is the venue. The distinction is architectural, not semantic.*

§4

What Is a Call. What Is a Put.

These are not textbook definitions. This is how calls and puts work in this specific instrument — through the AMM, with real swaps, no formula, no strike price.

CALL — BUYER BELIEVES XRP RISES	PUT — BUYER BELIEVES XRP FALLS
Deploy: seller deposits 100 XRP. AMM swaps to RLUSD at rate 0.50 → 50 RLUSD locked in escrow.	**Deploy:** seller deposits 100 RLUSD. AMM swaps to XRP at rate 0.50 → 200 XRP locked in escrow.
Settlement (XRP rose, rate 0.40): 50 RLUSD swaps back → 125 XRP. Seller gets 100 XRP (made whole). Buyer gets 25 XRP (gain).	**Settlement (XRP fell, rate 0.60):** 200 XRP swaps back → 120 RLUSD. Seller gets 100 RLUSD (made whole). Buyer gets 20 RLUSD (gain).
Settlement (XRP fell, rate 0.60): 50 RLUSD swaps back → ~83 XRP. Shortfall of ~17 XRP comes from buyer's margin.	**Settlement (XRP rose, rate 0.40):** 200 XRP swaps back → ~80 RLUSD. Shortfall of ~20 RLUSD comes from buyer's margin.

THE MECHANISM

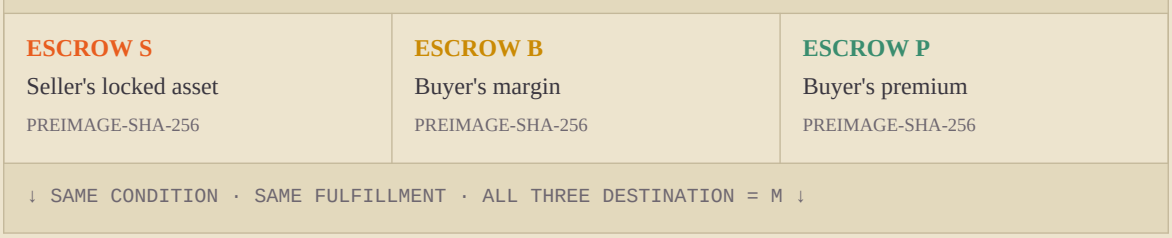
In both cases the seller is made whole first. The AMM determines the outcome. No oracle computes the difference. The swap itself is the settlement. The payoff is option-shaped — premium, margin, asymmetric exposure — but the mechanism is a spot trade, not a formula. There is no strike price. There is no payoff curve computed against a reference rate.

§5

The Escrow Primitive

A time-locked, condition-gated escrow with a cryptographic release mechanism does what a clearinghouse does: hold assets, prevent premature withdrawal, release on defined conditions. But the escrow is not an intermediary. It is a ledger object. Nobody operates it. Nobody can modify it after creation. The assets sit on-chain, owned by the creator, released only when the condition is met or the time expires.

FIG. 01 — THREE-ESCROW STRUCTURE WITH PER-CONTRACT MULTISIG



M — 2-of-2 MULTISIG · MASTER KEY DISABLED
Per-contract. Created at deploy. Cleaned up after settlement. Holds funds only during settlement transitions. Both parties must co-sign every distribution.

Three escrows with a shared cryptographic condition, pointed at a 2-of-2 multisig with its master key disabled, replicate the function of a clearinghouse without requiring one. The chain enforces custody. The condition enforces timing. The multisig enforces bilateral agreement.

If the coordination layer fails permanently, escrows hit their **CancelAfter** date and refund to their sources. Seller gets their deposit back. Buyer gets margin and premium back. Nothing is stuck. The failsafe is built into the ledger primitive, not into the software.

§6

Settlement Through the AMM

At deploy, the seller's asset is swapped through the AMM into its opposite. At settlement, it swaps back. The difference between what went in and what comes out is the contract's outcome. There is no formula. There is no computation against an external price.

DEPLOY	SETTLEMENT
Seller's 100 XRP → AMM swap → 50 RLUSD 50 RLUSD → Escrow S (destination M) RATE AT DEPLOY: 0.50 XRP/RLUSD	Escrow S releases 50 RLUSD into M 50 RLUSD → AMM swap → 125 XRP Seller receives 100 XRP · Buyer receives 25 XRP RATE AT SETTLEMENT: 0.40 XRP/RLUSD

> *There is no strike price. There is no payoff formula. There is a swap at deploy and a swap at settlement. The difference between those two swaps is the contract's outcome. That is simpler than every other option ever built.*

§7

Margin and the Two Tiers

The buyer's margin is their risk capital. It absorbs losses when the swap-back produces less than the seller's deposit. The margin is locked at deploy and cannot be topped up. The buyer knows their maximum loss before they sign: **premium plus margin. That is it.**

Soft liquidation at 90%

Both parties must agree. The buyer still has a 10% buffer. There is time. The buyer may believe the rate recovers. The seller is protected by the buffer while waiting for signatures. This tier preserves the buyer's agency over the timing of liquidation.

Hard liquidation at 100%

Automatic. No cooperation required. A pre-signed transaction fires. The buyer's margin is fully consumed. Waiting any longer means the seller's deposit starts eroding. The pre-signed swap-back delivers a fixed amount — **(deposit minus margin)** — to the seller.

ZONE	MARGIN CONSUMED	MECHANISM	BUYER AGENCY
Cooperative	0 – 90%	Both co-sign live	Full — can request voluntary close
Buffer	90 – 100%	Soft liquidation, co-signed	Limited — 10% buffer returned
Automatic	**100%+**	Pre-signed fires	None — margin fully consumed

THE DESIGN DECISION

The 90% threshold requires trust. The 100% threshold requires math. That boundary — where cooperation gives way to automation — is the design decision that makes the instrument functional for both parties.

§8

Why the Seller Cannot Cheat

The seller runs the bot. The bot holds the pre-signed liquidation transaction. The seller could fire it at any time after escrow release. But the pre-signed transaction delivers a fixed amount: **(deposit minus margin).** At any rate better than the 100% threshold, that amount is less than what the seller would get by waiting for a normal settlement.

MARGIN CONSUMED	AMM NEEDS	SELLER GETS	LEFT IN M	VS. WAITING
0% (no movement)	~90 of 100 RLUSD	90 XRP	~10 RLUSD	**−10 XRP value**
50% consumed	~95 of 100 RLUSD	90 XRP	~5 RLUSD	**−5 XRP value**
90% consumed	~99 of 100 RLUSD	90 XRP	~1 RLUSD	**−1 XRP value**
100% (intended)	100 of 100 RLUSD	90 XRP	0	**correct outcome**

> *The chain does not prevent the seller from firing early. The math makes it irrational. The protection is not enforcement. It is incentive alignment. The buyer is not trusting the seller to behave well. The buyer is trusting the seller to act in their own economic interest. That is a different kind of trust — one with a formal basis.*

§9

What Changes

DOMAIN	BEFORE	AFTER
Custody	Intermediary holds assets during the term	Escrow holds assets. Both wallets retain signing authority. No intermediary.
Price	Oracle feeds price to settlement formula	AMM executes a real swap. The rate is the outcome, not an input.
Settlement	Computed against external price. Synthetic delivery.	Executed through the market. Real assets, real swap, real outcome.
Liquidation	Protocol-controlled or manual	Two-tier: cooperative at 90%, automatic at 100%. Game-theoretic protection.
Borrowing	Required. Leverage through lending pools.	None. Both sides fully collateralised. Self-contained.
Infrastructure	Protocol, smart contracts, governance tokens, liquidity pools	Two wallets, three escrows, one multisig. Native ledger primitives. No protocol.

THE CONCLUSION

A self-custody option is not an option without a clearinghouse. It is an option where the ledger is the clearinghouse. The escrow holds custody. The AMM settles. The multisig enforces bilateral agreement. The game theory prevents abuse. No oracle. No pool. No borrowing. No protocol. What remains is the instrument itself — two parties, one pair, one term, one outcome determined by a real swap on a real market. That is what an option has always been. Everything else was infrastructure.

The architecture described in this paper is implemented in Caput. Two wallets. Three escrows. One multisig. One AMM. No oracle. No pool. No protocol. Self-custody options on XRP/RLUSD. This paper describes the why. caput.dev is the what.

Research conducted and architecture developed by Shane Calder, April 2026. Developed in collaborative reasoning with Anthropic Claude. This paper is a living document and will be updated as the architecture develops.

This paper describes a problem class and its resolution. It does not describe implementation. The architecture that addresses the problem class is the subject of separate work.