ShortVol / LongVol Proposed Specs

EPOCH	UNDERLYINGS	COLLATERAL
Seven days, settled in USDC	BTC and ETH	A USDC Pot held inside ShortVol

WHY THE STRUCTURE SHOULD CHANGE

I suggest we change the option construction structure, and here is why. The first reason is where the cash sits. The current version we are working with builds both tokens from calls: ShortVol owns a call at 80% and a call at 120% and has sold calls at 95% and 105%, which is a bought call condor, and LongVol holds the exact opposite. A bought position can never owe anything, so under that construction ShortVol is a pure asset with nothing behind it, and it is LongVol, the sold position, that has to hold the collateral. That puts the cash on the wrong token. ShortVol is the one that earns the premium and the one its holders would think of as the yield side, yet any yield on the idle collateral would flow to the ticket buyers, and the writer's role would sit with the token that is meant to be the cheap punt.

Building the same payoff as an iron condor, a written put spread below the market and a written call spread above it, fixes that without changing a single settlement value. ShortVol sells a put at 95% and buys one at 80%, sells a call at 105% and buys one at 120%, so it is now the writer of both spreads and holds the Pot, exactly as the Inverse and Short Put tokens already do, while LongVol buys both spreads and holds nothing, which is what a ticket should look like. A standard result of option pricing, put-call parity, makes the two constructions worth the same at every moment, so the engine's prices, the settlement table and the redemption rule are untouched, and any yield on the cash goes to the holders who want yield. Figure 1 shows the payoff that both constructions produce.

I also looked at whether the two tokens could be made equally likely to win, since at normal volatility ShortVol wins about three weeks in four and LongVol one. Even odds are possible, but only in two ways. The strikes can be pulled inside a typical weekly move, with the wings about 7% away on BTC, which turns both tokens into a coin flip on whether the week moves more than about 4.5% and leaves ShortVol wiped out roughly one week in four instead of one in eighty. Or the epoch can be stretched to a month, where the same strikes reach even odds at about 67% volatility. The monthly route creates an overlap with RiskON and RiskOFF, which settle on the same monthly clock and ask the same question about the month ahead: a RiskOFF holder expecting a quiet month is the natural ShortVol buyer, and a RiskON buyer who wants a big move without a strong view on direction would drift to LongVol, because LongVol pays either way while RiskON only pays on the upside. The lopsided weekly pair is therefore deliberate. It keeps ShortVol a rarely wiped-out yield token, keeps LongVol a cheap ticket, and keeps both out of RiskON and RiskOFF's lane.

The second reason is the currency of the collateral. The payouts should be fixed in dollars at the start of the week, so the Pot has to be dollars too: a Pot held as 0.15 BTC is worth only $14,400 when $15,000 is owed if BTC slips from $100,000 to $96,000, so deposits in the underlying should not be included. The third reason is the epoch. A weekly epoch gives both tokens a natural buyer, the range seller on one side and the event trader on the other, and it keeps the pair on a different clock from RiskON and RiskOFF, whose monthly rhythm a monthly condor would compete with. I also tested strikes that move with the volatility forecast and rejected them; section 5 explains why.

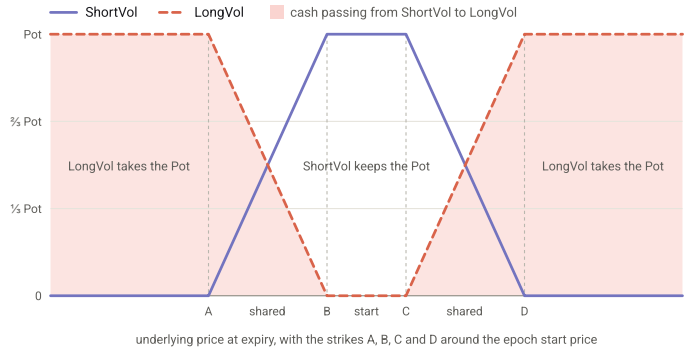


Figure 1. What each token is worth at the end of the week, in either construction. ShortVol keeps the Pot between B and C and is worth nothing beyond A or D; LongVol is the mirror image, and the shaded area is the cash that passes from ShortVol to LongVol. On BTC the strikes A, B, C and D are 80%, 95%, 105% and 120% of the starting price; on ETH they are 70%, 95%, 105% and 130%.

1 What the pair is

A trader deposits USDC equal to the Pot with TRP and receives two tokens in return, one ShortVol and one LongVol. The Pot is the only money the pair ever holds, because the two tokens are exact opposites of each other on a set of options that pay out only at expiry, at the end of the week. Whatever the underlying does, ShortVol's value plus LongVol's value equals the Pot at every moment, and one of each token can always be handed back for the Pot.

The Pot is 15% of the underlying's starting price for BTC and 25% for ETH, and those two numbers are not chosen on their own. Each is the distance between the outer and inner strikes, 95% minus 80% on BTC and 95% minus 70% on ETH, which is the most the options can ever pay out, so the Pot is exactly the largest claim the pair can produce. ETH's wing sits further out because ETH moves more. Over the last three years a typical week has moved 6.4% on BTC and 9.3% on ETH, so a wing at 20% on BTC sits about three typical moves away and a wing at 30% on ETH a little over three. Measured on actual weeks, BTC ended beyond 20% in 1.3% of weeks over that period and ETH beyond 30% in 1.0%, whereas ETH beyond 20% happened in 4.0% of weeks, three times as often; over six years the same three figures are 3.6%, 1.8% and 6.5%. The model at current volatility says much the same, a total loss for ShortVol in 0.26% of BTC weeks and 0.14% of ETH weeks on the chosen ladders. The wider ETH wing therefore buys ETH's ShortVol the same rarity of total loss that BTC's has, at the cost of a bigger Pot per pair.

The simplest way to hold the pair in mind is as a weekly lottery on a large move. LongVol is the ticket. It costs about a tenth of the Pot at normal BTC volatility, is worth nothing in most weeks, and pays up to nine times its price when the week breaks out beyond the wings, in either direction. ShortVol is the house that sells the ticket. It holds the whole jackpot in cash, keeps the ticket money in every quiet week, pays out part of the jackpot on a moderate move and all of it on a large one. What makes the house safe is that the jackpot is capped at the Pot and funded in full before the week starts, so ShortVol can never owe more than it holds, and nobody borrows or posts margin. The difference from a real lottery is that the odds are not set by a machine but by how much the market moves, and the ticket price is set each week by the engine's forecast of exactly that.

WORKED EXAMPLE, BTC

BTC starts the week at $100,000 and the engine forecasts 47% annualised volatility for the week ahead. A minter deposits $15,000 and receives one ShortVol and one LongVol. Here is how the engine arrives at $13,352 for ShortVol and $1,648 for LongVol.

Step 1, turn the forecast into a weekly move. Volatility is quoted per year and a week is 7/365 of a year, so the typical weekly move is 47% × √(7/365) = 47% × 0.138 = 6.5%. On $100,000 that is a typical move of about $6,500 in either direction.

Step 2, draw the range of outcomes. With a typical move of 6.5%, the model's bell curve (Figure 3) gives BTC a 22.5% chance of ending the week below $95,000, a 21.7% chance of ending above $105,000, a 0.03% chance of ending below $80,000 and a 0.2% chance of ending above $120,000. It also says where BTC ends on average in each case: when it finishes below $95,000 it finishes at $91,539 on average, a shortfall of $3,461, and when it finishes above $105,000 it finishes at $109,032 on average, an excess of $4,032.

Step 3, value each option. An option is worth the chance that it pays multiplied by its average payout when it does, so the $95,000 put is worth 22.5% × $3,461 = $779 and the $105,000 call is worth 21.7% × $4,032 = $875. The two wing options are worth almost nothing because a 20% move in a week is about three typical moves, which the bell curve treats as very rare.

OPTION	CHANCE IT PAYS	AVERAGE PAYOUT WHEN IT PAYS	VALUE
Put at $95,000	22.5%	$3,461	$779
Put at $80,000	0.03%	$1,320	$0.45
Call at $105,000	21.7%	$4,032	$875
Call at $120,000	0.2%	$2,349	$5

Step 4, add up LongVol. LongVol owns the $95,000 put and has sold the $80,000 put, so its put spread is worth $779 − $0.45 = $778. It owns the $105,000 call and has sold the $120,000 call, so its call spread is worth $875 − $5 = $870. Together LongVol is worth $1,648, and Figure 2 shows the four legs stacking up to that number.

Step 5, what is left is ShortVol. $15,000 − $1,648 = $13,352, which is 89% of the Pot, and LongVol is the other 11%. Real weeks reach the wings more often than the bell curve says, in 1.3% of BTC weeks between 2024 and 2026 against 0.3% in the model, and the engine layers a tail adjustment on top of the forecast for exactly that reason.

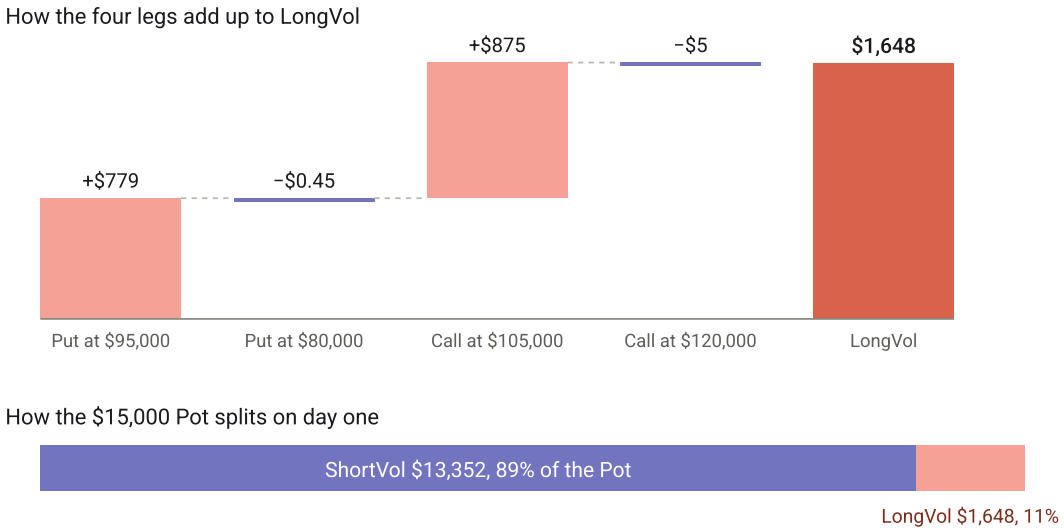


Figure 2. The engine's arithmetic for the example. The two bought options add value, the two sold ones take a little away, and the result is LongVol's price; whatever is left of the Pot is ShortVol's.

WORKED EXAMPLE, BTC, CONTINUED

Step 6, what each holder makes. The minter keeps the token they want and sells the other, so ShortVol buyers put up $13,352 and LongVol buyers $1,648, and the whole $15,000 sits inside ShortVol for the week. If BTC ends at $103,000, inside the band, ShortVol keeps the $15,000: $15,000 ÷ $13,352 = 1.123, a return of 12.3% on what its holder paid, while LongVol expires worthless. If BTC ends at $125,000 or $70,000, ShortVol pays the whole $15,000 to LongVol, and $15,000 ÷ $1,648 = 9.1, so the ticket has paid 9.1 times. If BTC ends at $90,000, ShortVol pays $5,000 and keeps $10,000, a loss of 25% on $13,352, while LongVol turns $1,648 into $5,000, a gain of 203%.

Step 7, how the forecast moves the split. The same arithmetic with a 30% forecast, a typical move of 4.2%, opens ShortVol at $14,536 and LongVol at $464, so the ticket costs 3% of the Pot and pays up to 32 times. With a 64% forecast, a typical move of 8.9%, ShortVol opens at $11,921 and LongVol at $3,079, so the ticket costs 21% of the Pot and pays up to 4.9 times. The wider the market is expected to swing, the more the ticket costs and the more ShortVol earns for carrying it.

> The volatility figures used in this document's examples are approximate. They come from a simple forecast built on Coin Metrics prices, chosen to make the mechanics easy to visualise; the engine's own forecast will differ slightly, and so will the exact opening prices.

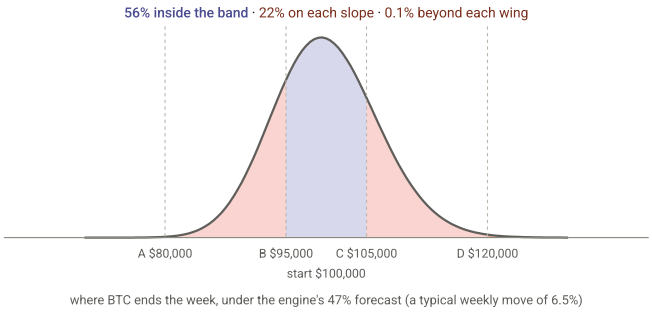


Figure 3. Where the model expects the week to end at 47% volatility. More than half of the probability sits inside the band, where ShortVol keeps the Pot; most of the rest sits on the slopes, where the Pot is shared; only 0.2% sits beyond the wings, where LongVol takes it all. ShortVol's opening price is the Pot less the probability-weighted claim, which is why it opens at 89% of the Pot.

2 The week

Each epoch runs for seven days. The proposed expiry is Friday 08:00 UTC, the moment at which the weekly listed options that market makers already hedge expire, so that ShortVol and LongVol can be priced and hedged against instruments that exist. At the start of each week TRP publishes the start and end times, the four strikes, the Pot and the engine's forecast, and the pair is then open for minting, redemption and trading all week. At expiry the tokens are settled in USDC and a fresh series is created for the following week, with strikes reset around the new starting price; section 8 sets out how settlement and rolling work.

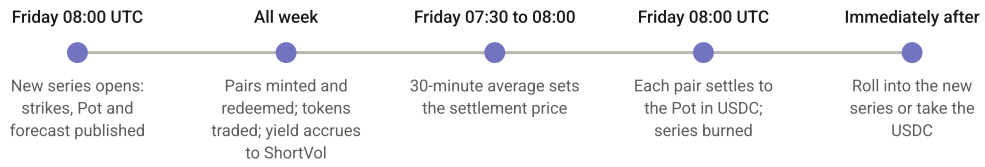


Figure 4. One week in the life of a series. The same clock repeats every Friday, so a holder who rolls is always in a series with strikes set around the latest price.

3 ShortVol

ShortVol consists of the USDC Pot plus a written put spread below the market and a written call spread above it: it has sold a put at Strike B and bought one at Strike A, and sold a call at Strike C and bought one at Strike D. Traders call this a cash-secured iron condor, the position a volatility seller uses when they want a known maximum loss. Between B and C both spreads expire worthless and ShortVol keeps the full Pot. Below B the put spread pays out point for point until A, above C the call spread pays out until D, and beyond A or D everything has been paid out and ShortVol is worth nothing. At any moment its value is the Pot less what the two spreads it has written are currently worth, which is the same as the Pot less LongVol's value.

> ShortVol value = Pot − (value of the put spread + value of the call spread) = Pot − LongVol value, always between 0 and the Pot

The Pot sits inside ShortVol because ShortVol is the side that can owe, and because the Pot equals the largest combined payout of the two spreads, ShortVol is never asked for more than it holds. While it waits, the Pot can earn stablecoin yield, which goes to ShortVol (section 7). The name describes the position: the holder is short volatility, and earns the premium built into the opening price in every week that stays calm enough.

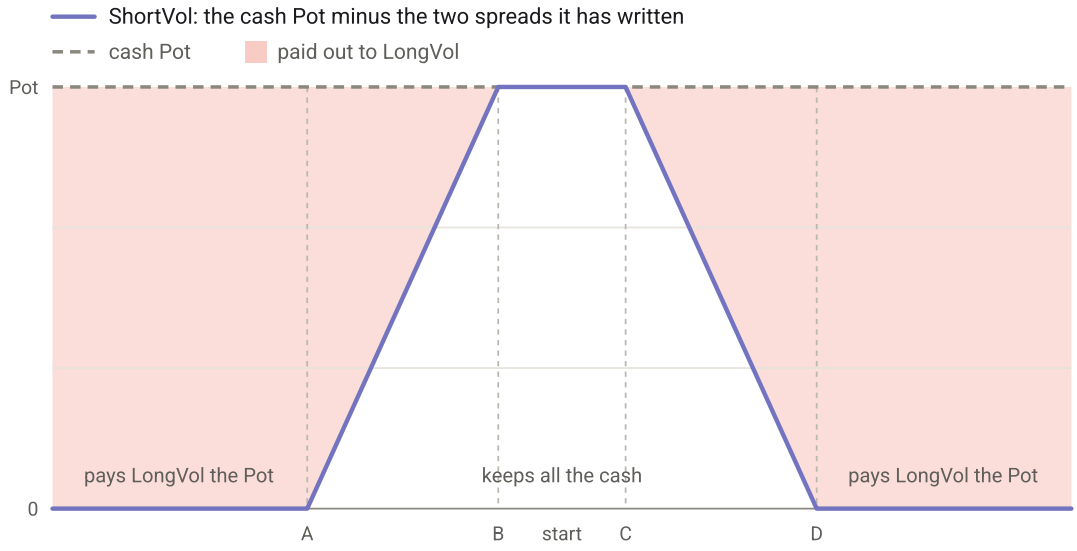


Figure 5. ShortVol on its own. The dashed line is the cash Pot it holds, and the shaded area is what it pays out as the spreads it has written come into the money; between B and C it pays nothing and keeps everything.

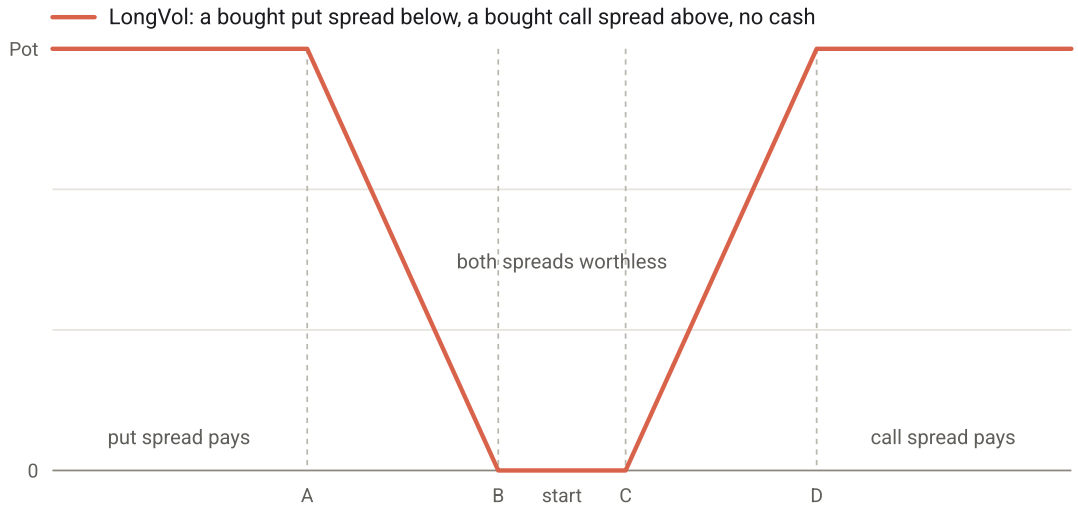


Figure 6. LongVol on its own. Nothing but the two bought spreads, the put spread paying on the left and the call spread on the right, with no cash behind them because a bought spread can only receive.

4 LongVol

LongVol consists of a bought put spread below the market and a bought call spread above it: it has bought a put at Strike B and sold one at Strike A, and bought a call at Strike C and sold one at Strike D. It is the ticket that ShortVol has sold. It gains value as the underlying moves away from its starting price in either direction, is worth the whole Pot at or beyond A or D, and is worth nothing between B and C. It holds no collateral because it can only ever receive; going to zero means receiving nothing, never owing anything.

> LongVol value = value of the put spread + value of the call spread = Pot − ShortVol value, always between 0 and the Pot

Both tokens are priced in USD. This construction gives the same token values at every moment as the all-call condor in the current version, a standard result of option pricing, so only the location of the cash and the identity of the writer change.

5 The strikes and the Pot

The strikes are fixed percentages of the underlying's starting price and are reset around the new price every week. The inner strikes, which set the band, are the same on both underlyings; the outer strikes, which set the wings, are placed per underlying so that ShortVol is wiped out about as rarely on ETH as on BTC.

PARAMETER	BTC	ETH	NOTES
Strike A (bought put in ShortVol)	80% of start	70% of start	Lower wing; ShortVol is worth nothing at or below it
Strike B (sold put in ShortVol)	95%	95%	Lower edge of the band
Strike C (sold call in ShortVol)	105%	105%	Upper edge of the band
Strike D (bought call in ShortVol)	120%	130%	Upper wing; ShortVol is worth nothing at or above it
Pot per pair	15% of start	25% of start	The distance from B to A, and from C to D; held in USDC
Epoch	7 days	7 days	Expiry proposed at Friday 08:00 UTC
Option style	Pays only at expiry	Pays only at expiry	European style

Because the ladder is fixed while the size of a typical weekly move rises and falls with the market, the pair changes character as volatility changes. In a calm market the band is wide compared with the moves being made, so ShortVol earns a small premium almost without risk and LongVol is a long-odds ticket. In a wild market the band is narrow compared with the moves, so ShortVol earns a large premium and is wiped out far more often, and LongVol wins two

weeks in five. Figure 7 draws the two sides of that trade-off for the BTC ladder, and the table gives the model values at the volatility levels that matter, assuming the forecast turns out to be right.

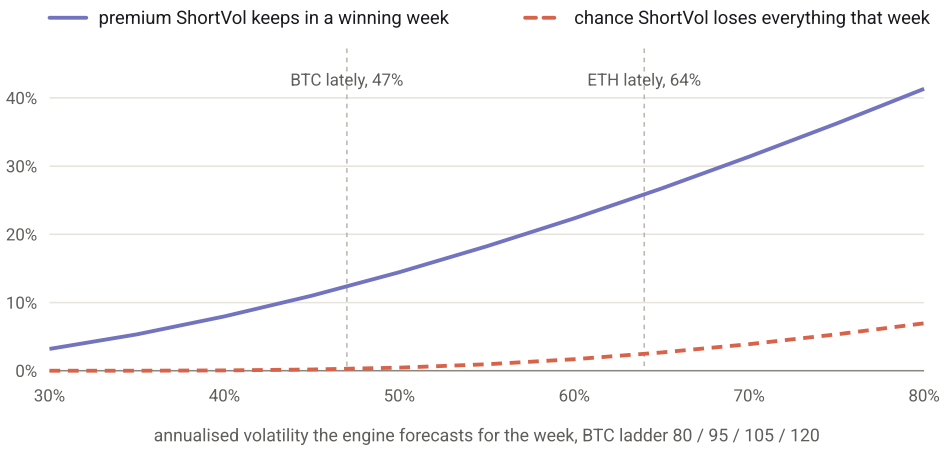


Figure 7. What a fixed ladder does as volatility changes. The premium ShortVol keeps in a good week rises from 3% at 30% volatility to 41% at 80%, and the chance of losing everything in a given week rises from almost nil to 7% over the same range.

ANNUALISED VOLATILITY	TYPICAL WEEKLY MOVE	SHORTVOL OPENS AT	PREMIUM IN A WINNING WEEK	TOTAL-LOSS CHANCE PER WEEK	LONGVOL WINS	LONGVOL MAX PAYOUT
BTC 30%	4.2%	97% of Pot	3.2%	under 0.01%	19%	32x
BTC 47%	6.5%	89%	12.3%	0.26%	31%	9.1x
BTC 64%	8.9%	79%	25.8%	2.5%	36%	4.9x
BTC 80%	11.1%	71%	41.3%	7.0%	40%	3.4x
ETH 47%	6.5%	93%	7.1%	under 0.01%	31%	15x
ETH 64%	8.9%	87%	14.5%	0.14%	36%	7.9x
ETH 80%	11.1%	81%	23.0%	0.85%	38%	5.3x

Why the strikes should stay fixed

The obvious alternative is to let the strikes move with the forecast, so that the wings always sit three typical moves away and the odds look the same every week. It sounds fairer, and it tests worse, and a single calm week shows why. Suppose the forecast is 30%, a typical move of 4.2%, so moving strikes would put the wings 12.5% away, at $87,500 and $112,500 with BTC at $100,000. The forecast is built from recent weeks and cannot see a shock coming. When a 15% week arrives, the kind that has happened in 3.4% of BTC weeks over the last three years, it goes straight through the moving wing and ShortVol loses everything. With the wing fixed at 20%, at $80,000 and $120,000, the same 15% week costs ShortVol two thirds of the Pot and leaves it a third, and it takes a 20% week, which has happened in 1.3% of weeks, to wipe it out.

6 Minting and redeeming

A pair comes into existence when a trader deposits USDC equal to the Pot and receives one of each token, which can happen at any time during the week at the current values, so that every pair in a series carries the same strikes and the same expiry however late it was minted. It goes out of existence when a trader returns one of each token and receives the Pot back, together with whatever yield has accrued on it. The Pot is held inside ShortVol, whose written spreads are its liability, and LongVol holds nothing, but economically the two sets of buyers supply the Pot between them in proportion to their tokens' opening values. At 47% volatility on BTC, ShortVol buyers supply about 89% of every Pot and LongVol buyers about 11%, roughly eight to one, and at 64% on ETH the ratio is about seven to one. The ratio narrows when volatility rises because LongVol becomes dearer, and it means that every dollar of LongVol demand supports seven to eight dollars of ShortVol, which makes LongVol demand the practical limit on how large the market can be.

WORKED EXAMPLE, ETH

ETH starts the week at $2,500 with a 64% forecast, a typical weekly move of 8.9%. The Pot is $625 and the strikes are $1,750, $2,375, $2,625 and $3,250. The engine values the $2,375 put at $37.68 and the $2,625 call at $41.45, and the two wing options at almost nothing, so LongVol is worth $79 and ShortVol $546. A market maker who mints ten pairs for $6,250, sells the ten ShortVol to a yield desk for $5,460 and the ten LongVol to event traders for $790 has recovered the deposit, and the $6,250 sits inside the ten ShortVol tokens for the week.

7 Yield on the Pot

The Pot need not sit idle. It can be deployed during the week into a whitelisted, instantly redeemable stablecoin lending market on the deployment chain, of the kind Aave v3 offers on Arbitrum, with an undeployed buffer so that redemptions of pairs can always be met on demand. If it is, the yield accrues daily to ShortVol's value, since ShortVol holds the cash, and is paid out with the Pot at settlement or redemption. At a lending rate of 4.5% a year the Pot earns about 0.09% a week, which is about $13 on a $15,000 BTC Pot, small for one holder but about $2.3 million a year on $50 million of Pots. The management fee that the TokenFactory already supports can be taken from this yield rather than from holders' balances, so that a 2% a year fee leaves roughly 2.5% a year to ShortVol holders at current rates.

8 Settlement and rolling

The settlement price should be the average of the Coin Metrics reference price over the last 30 minutes before expiry, the convention listed crypto options use, so that no single second's print can decide a week. At expiry each pair settles to the Pot: LongVol receives what its two spreads pay at the settlement price, ShortVol receives whatever remains, both in USDC, and the tokens of the expired series are burned. Figure 8 shows how the $15,000 BTC Pot divides across a range of closing prices, and the table gives the same outcomes as returns on what each holder paid.

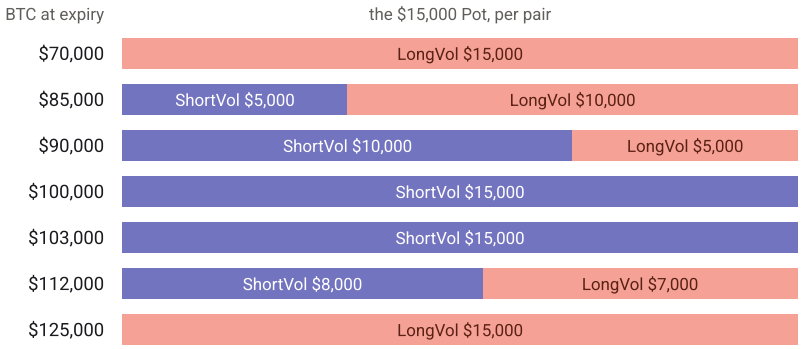


Figure 8. How one BTC Pot divides at settlement. Inside the band ShortVol keeps everything; on the slopes the Pot is shared point for point; beyond the wings LongVol takes it all.

BTC AT EXPIRY (START $100,000)	SHORTVOL RECEIVES	RETURN ON $13,352	LONGVOL RECEIVES	RETURN ON $1,648
$70,000, lower wing	$0	−100%	$15,000	+810%
$85,000, lower slope	$5,000	−63%	$10,000	+507%
$90,000, lower slope	$10,000	−25%	$5,000	+203%
$100,000, band	$15,000	+12.3%	$0	−100%
$103,000, band	$15,000	+12.3%	$0	−100%
$112,000, upper slope	$8,000	−40%	$7,000	+325%
$125,000, upper wing	$0	−100%	$15,000	+810%

Rolling is automatic. At settlement, whatever corpus a holder is left with is used to mint the new week's series, so every holder starts the next week holding new ShortVol and new LongVol in the pair ratio. A holder who wants only one leg sells the other on the marketplace at the opening value, and a holder whose token settled at zero has nothing to roll. Rolling happens by minting rather than by rebasing the old tokens in place, so each week starts clean, with strikes around the new price.

9 Users

Who holds ShortVol

ShortVol is for people who already sell volatility and want a defined-risk way to keep doing it: traders who sell weekly options or strangles on listed venues, liquidity providers whose range strategies already earn in a band and lose on a breakout, and market-neutral desks that harvest premium for a living. What it offers them is the largest weekly premium of any range strategy, a loss capped at the position with no margin and no liquidation, and a stablecoin yield on the collateral underneath. It is not a substitute for lending or fixed-rate yield, because it loses part of the position in about one week in four and all of it in about one week in eighty on BTC, and it belongs in a portfolio as a sleeve rather than as a treasury allocation.

Who holds LongVol

LongVol is for people who want a large move without having to guess its direction: event traders positioning into central bank weeks, inflation prints and ETF decisions, buyers of far out-of-the-money weekly options and weekly price-range bets who want a cheap ticket with a capped cost, and hedgers who are short gamma, above all concentrated liquidity providers and market makers, for whom a weekly wing that pays in either direction is inexpensive insurance. At 47% volatility on BTC the ticket costs about a tenth of the Pot and pays nine times in a wing week; at 64% on ETH it costs about an eighth and pays eight times. The one holder the design tries not to attract is a systematic volatility fund buying underpriced wings every week, which is what the engine's tail adjustment is there to prevent.

10 Risks

ShortVol

- Total loss: a week ending beyond Strike A or Strike D leaves ShortVol worth nothing. Over 2024 to 2026 that happened in about one BTC week in eighty and one ETH week in ninety on the chosen ladders, and one and a half to two and a half times as often over the six years from 2021.
- Partial loss: about one week in four ends on a slope, with a median loss near a fifth of the position.
- Correlated losses: the wing weeks are crashes and squeezes, so ShortVol loses at the same time as most other crypto positions and offers no diversification against them.
- Thin premium in calm markets: at 30% volatility the premium is about 3% a week, so a single wipe-out costs more than thirty winning weeks.
- Pricing and forecast risk: the premium depends on the engine's forecast and tail adjustment, and if the forecast runs low relative to what the market then does, ShortVol is under-compensated.
- Collateral venue risk: USDC deployed for yield is exposed to the lending market's contracts and liquidity; the undeployed buffer limits but does not remove this.

LongVol

- Losing is the usual outcome: LongVol loses money in about three weeks in four on BTC and expires worth nothing in about two weeks in three.
- Dead zone: a move that stays inside the band pays nothing, so a 4% week is a total loss even though the underlying moved.
- Time decay: LongVol's value falls as the week passes without a move.