pSymm

Private, Symmetrical derivatives

Market Context & Costs

Derivatives is the biggest financial product.

Around ~90% of derivatives volume is done over-the-counter.

Current OTC infrastructure costs:

- $50B/year
- Substantial business missed due to high latency and expensive products.

Challenge & Solution

Lack of privacy onchain is one of the biggest factor making blockchain unappealing for TradFi.

pSymm integrates Aztec L2 and an L1 dispute settlement system to enable privacy for collateralized trading sessions.

Market Opportunity

- 100x cost reduction enables 100x new market participants previously excluded by high costs.
- Network effect: Only one major bank needed to distribute multiple banks' OTC products through the platform.
- Small players who cannot access banks directly can join our network.
- Historical pattern: Every 100x cost reduction in technology creates massive market transformations.
- If one big bank provides products from other banks through our OTC, we de facto win.

Trading Session Flow

1. A trader connects to the solver's websocket.

Then the flow is symmetrical:

2. Deposit USDC to pSymm.nr on Aztec L2 (through TokenPortal).
3. Emit encrypted log to prove collateral.
4. Trade offchain, sign each message.

Scenario 1: Happy Path

Continuing the flow:

5. Cosign the collateral withdrawal (taking PnL into account).

Scenario 2: Dispute

Alternatively:

5. One of the parties disputes PnL, reveals offchain session.
6. SettleMaker (L1) validators automatically vote on resolution (based on trading rules)

Summary

It works because my trades are bilateral with my market maker - only my counterparty and I know about the trades.

In case of a dispute, API bug or hack, or for extra safety, I can reveal the trades to a network of KYC/AML entities, which settle disputes based on established rules.

If my counterparty lies about the trades during a dispute, all transactions have been signed, so I can prove that I am right.

Thank you for your attention.

Any questions welcome!