EIP-2537

Dark Pool Evolved

Trustless Randomness (VRF) using EIP-2537

(Precompile for BLS12-381)

Problem: MEV in Dark Pools

- Dark Pool as Private DEX
  - Challenge: transaction ordering affected fairness
- MEV (Miner Extractable Value)
  - Miners reorder or censor transaction to gain benefits

Need for Random Ordering

VRF (Verifiable Random Function)

- Tranditional Random
  - Off-chain: oracles
    - Need trust assumption
  - On-chain: generate & proof
    - Gas too high (without precompile)

May 7, 2025, Pectra (Prague) Upgrade

Better user experience:

- EIP-7702 - *Set EOA account code*
- EIP-7691 - *Blob throughput increase*
- EIP-7623 - *Increase calldata cost*
- EIP-7840 - *Add blob schedule to EL config files*

Better staking experience:

- EIP-7251 - *Increase the MAX_EFFECTIVE_BALANCE*
- EIP-7002 - *Execution layer triggerable exits*
- *eral purpose execution layer requests*
- *ly validator deposits on chain*

EIP-2537

Protocol efficiency and security improvements:

- EIP-2537 - *Precompile for BLS12-381 curve operations*
- EIP-2935 - *Save historical block hashes in state*
- EIP-7549 - *Move committee index outside Attestation*

EIP-2537 Precompile for BLS12-381 curve operations

Operation	EIP-1108 Gas (BN254)	EIP-2537 Gas (BLS12-381)
G1 Addition	150	375
G1 Multiplication	6,000	12,000
Pairing Check	34,000 × k + 45,000	32,600 × k + 37,700
G1 MSM	–	Dynamic
G2 Addition	–	600
G2 Multiplication	–	22,500
G2 MSM	–	Dynamic
Fp → G1 Mapping	–	5,500
Fp2 → G2 Mapping	–	23,800

Enable on-chain VRF

Dark Pool Trading Privacy-Preserving

Create Identity ● 0xb534...38e8 ● Matching

Place Order

Current Epoch Progress

Block 2 / 5 matching ● Matching...

ETH-USD

Price	24h Change
$4025.50	+1.65%

Liquidity	Spread
High	≈ 4022.5 - 4026.5 USD

Place Order

● Identity Required

Buy | Sell

Limit | Market

Amount (ETH)

0.0000

Price (USD)

Trading Activity

Trading Activity by Epoch

Recent epochs with orders

Epoch #56 matching 15 orders 15 pending

Pending Orders

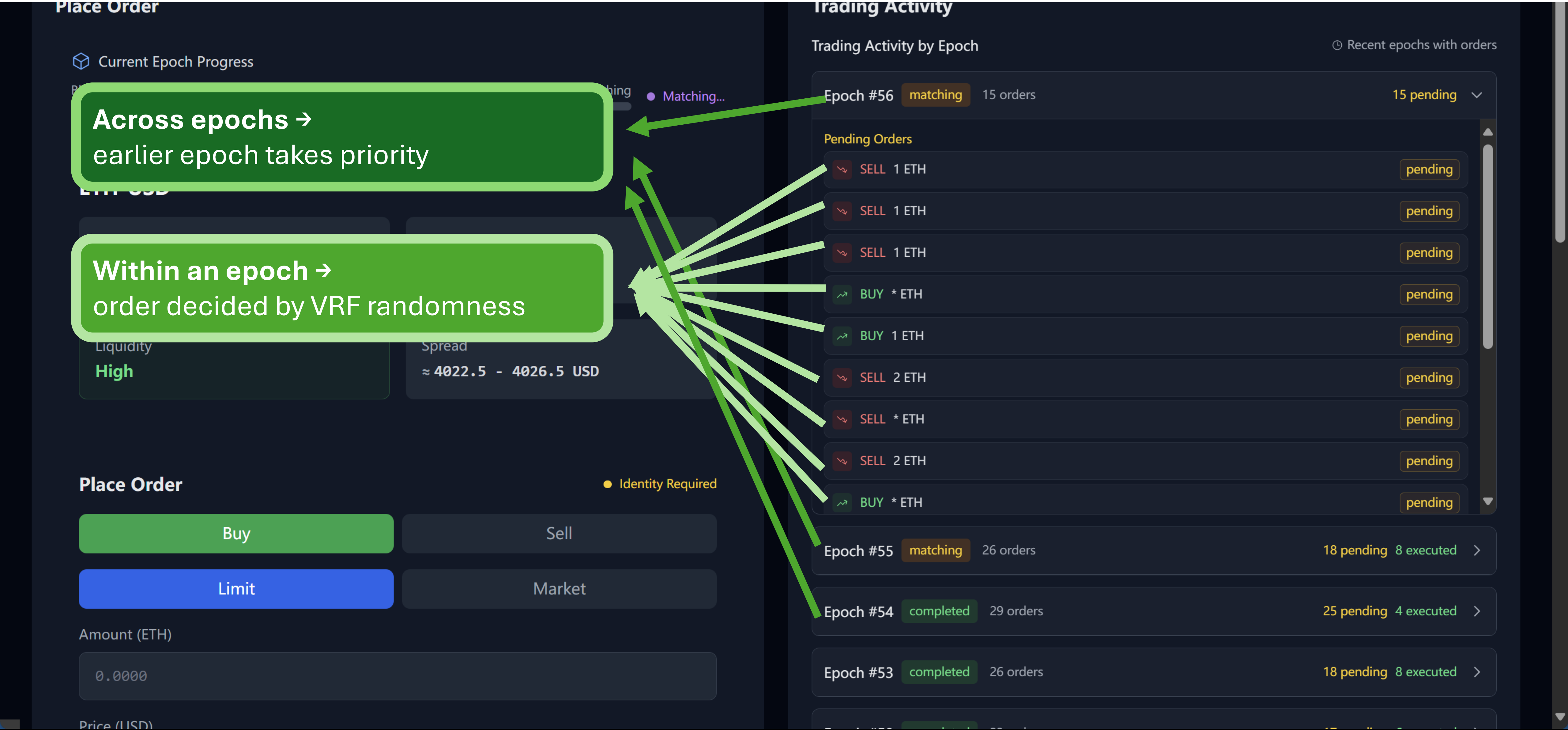
SELL	1 ETH	pending
SELL	1 ETH	pending
SELL	1 ETH	pending
BUY	* ETH	pending
BUY	1 ETH	pending
SELL	2 ETH	pending
SELL	* ETH	pending
SELL	2 ETH	pending
BUY	* ETH	pending

Epoch #55 matching 26 orders 18 pending 8 executed

Epoch #54 completed 29 orders 25 pending 4 executed

Epoch #53 completed 26 orders 18 pending 8 executed

Epoch-based Ordering



DEMO

Prover
(Typescript)

- **Input:** sk, pk, in
  where sk is the private key used to generate the signature and randomness output, and in is the input.

  1. Compute

     $$preout = sk \cdot H_{\mathbb{G}}(in)$$

     where $H_{\mathbb{G}}$ is the hash-to-curve operation and H is a general hash function.

  2. Select a random scalar $r_1 \in \mathbb{F}_p$.

  3. Compute

     $$R = r_1 \cdot G$$

     $$R_m = r_1 \cdot H_{\mathbb{G}}(in)$$

  4. Compute

     $$c = H_p(in, pk, preout, R, R_m)$$

     where H_p is a hash mapped into the finite field $\mathbb{F}_p$.

  5. Compute

     $$s_1 = r_1 + c \cdot sk$$

- **Output:** $c, s_1, preout$

Verifier (Solidity)

1. Compute

$$R = s_1 \cdot G - c \cdot pk$$

$$R_m = s_1 \cdot H_{\mathbb{G}}(in) - c \cdot preout$$

2. Verify

$$c \stackrel{?}{=} H_p(in, pk, preout, R, R_m)$$

3. If the equality holds, compute

$$out = H(preout, in)$$

and output *out*; otherwise, output **false**.

Proof of Work