LAUREL

LAUREL: Verifiable Parimutuel Rounds on a 5×5 Grid

Threshold-BLS randomness, on-chain verification, and the economics of mining by covering cells

Whitepaper v0.1 · November 2026 · Elysium (Hyperliquid L2)

Abstract

LAUREL is a game of rounds played on a grid of 25 cells. During a fixed betting window players stake HYPE on any subset of cells. When the window closes, a public threshold-BLS beacon (drand) selects one winning cell; its signature is verified on-chain over the BN254 pairing, so no operator, keeper or validator can choose the outcome. Players on the winning cell share every other cell's stake minus a protocol fee, pro rata, together with the round's emission of the LAUREL token, and with probability $1/625$ an accumulated jackpot. We specify the timing rule that makes the beacon unknowable while bets are open, bound the bias of the cell selection by 5.3×10^{-77} in total variation, derive the exact payout map and its conservation properties, and analyse the game as a parimutuel market. Two results shape play: the expected fee of a round equals $\frac{24}{25}\varphi T$ regardless of how the book is distributed, and any uncovered cell is strictly profitable to cover. Under free entry, the fees paid by participants who cover the board converge to the market value of the tokens they mine.

1 Overview

Every round has the same life cycle. Bets are open for W seconds; then the round enters a break of $P - W$ seconds in which no bets are accepted, the beacon is published, anyone settles the round on-chain, and the next round begins. With the deployed parameters $P = 75$ s and $W = 60$ s there are $86\,400/P = 1152$ rounds per day.

1. **Bet.** A player sends HYPE together with a list of cells and amounts. Each amount is at least the minimum stake $s_{\min}$. A player may bet several times per round and on as many cells as they like.
2. **Close.** At the close time c_r the contract stops accepting bets for round r. This is enforced by the contract, not by the interface.
3. **Draw.** The first drand beacon produced strictly after c_r determines the winning cell and whether the jackpot fires.
4. **Settle.** Anyone may submit the beacon signature. The contract verifies it, computes the winning cell, fixes the pot and the token pool, and books the protocol fee.
5. **Claim.** Winners claim HYPE and newly minted LAUREL for any number of rounds in one transaction. If a round is not settled within $\Delta = 3600$ s of its close, every stake becomes refundable in full.

2 Notation

Symbol	Meaning	Value / source
$t_0,\ P,\ W$	start time, round period, betting window	immutable; $P = 75$ s, $W = 60$ s
$c_r = t_0 + rP + W$	close time of round r	`roundEnd(r)`
$g,\ p$	drand evmnet genesis and period	1 727 521 075, 3 s
$n_r,\ \sigma_n$	beacon round used by round r; its signature	`drandRoundFor(r)`
ρ_r	randomness of round r	$\mathrm{SHA256}(\sigma_{n_r})$
$w_r,\ J_r$	winning cell, jackpot indicator	§4
$s_{i,k}$	stake of player i on cell k	wei of HYPE
$S_k,\ T,\ u_i$	stake on cell k, round total, player total	$S_k = \sum_i s_{i,k}$, $T = \sum_k S_k$, $u_i = \sum_k s_{i,k}$
φ	fee rate, locked at the round's first bet	$\varphi \le 0.15$; default 0.10
$e,\ j$	LAUREL emission per round, jackpot accrual per round	set at deployment
$\mathcal{M}_r$	jackpot pool when round r settles	`motherlodePool`
$K^+,\ K^0$	cells with $S_k > 0$, cells with $S_k = 0$	$\lvert K^+\rvert + \lvert K^0\rvert = 25$

3 Round timing

Round r is open on the half-open interval $\mathcal{O}_r = [\,t_0 + rP,\ c_r)$ with $c_r = t_0 + rP + W$, and a bet sent at block time t is booked into round $\lfloor (t - t_0)/P \rfloor$ only if $t \in \mathcal{O}_r$. The beacon assigned to the round is

$$n_r \;=\; \left\lfloor \frac{c_r - g}{p} \right\rfloor + 2, \qquad \tau(n) \;=\; g + (n-1)\,p, \tag{1}$$

where $\tau(n)$ is the time at which drand round n is produced.

Lemma 1 (the beacon follows the close). *For every round r, $c_r \;<\; \tau(n_r) \;\le\; c_r + p$.*

Proof. Write $c_r - g = ap + b$ with $a = \lfloor (c_r - g)/p \rfloor$ and $0 \le b < p$. Then $\tau(n_r) = g + (a+1)p = c_r + (p - b)$, and $0 < p - b \le p$. □

Every bet of round r is therefore placed while the signature σ_{n_r} does not yet exist: no subset of drand nodes large enough to produce it has signed round n_r. The draw follows the close by at most one beacon period, so the break of $P - W = 15$ s comfortably contains publication, settlement and the animation of the result.

4 Randomness

4.1 Threshold BLS on BN254

The drand *evmnet* network runs the scheme `bls-bn254-unchained-on-g1`. Let $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ be the groups of prime order q of the BN254 curve with generators g_1, g_2 and the optimal Ate pairing $e : \mathbb{G}_1 \times$

$\mathbb{G}_2 \to \mathbb{G}_T$, which is bilinear and non-degenerate. The network holds a secret $x \in \mathbb{Z}_q$ shared among N nodes with threshold t; the group public key is $\mathrm{PK} = x\,g_2 \in \mathbb{G}_2$. For round n the message and signature are

$$m_n = \mathrm{keccak256}\big(\mathrm{be}_{64}(n)\big), \qquad \sigma_n = x \cdot H(m_n) \in \mathbb{G}_1, \tag{2}$$

where H hashes to $\mathbb{G}_1$ with `expand_message_xmd` over keccak-256 and the Shallue–van de Woestijne map, under the domain separation tag `BLS_SIG_BN254G1_XMD:KECCAK-256_SVDW_RO_NUL_`. The scheme is *unchained*: m_n depends on n alone, so any round can be verified without its predecessors. Each node i publishes a partial signature $\sigma_n^{(i)} = x_i H(m_n)$, and any t of them interpolate in the exponent:

$$\sigma_n \;=\; \sum_{i \in S} \lambda_i\, \sigma_n^{(i)}, \qquad \lambda_i = \prod_{j \in S,\, j \neq i} \frac{j}{j - i} \bmod q, \qquad |S| = t. \tag{3}$$

The contract accepts a 64-byte σ only if the pairing equation holds, checked with the EIP-197 precompile:

$$e(\sigma,\; g_2) \;=\; e\big(H(m_{n_r}),\; \mathrm{PK}\big). \tag{4}$$

Lemma 2 (uniqueness). *For fixed* PK *and* n *there is exactly one* $\sigma \in \mathbb{G}_1$ *satisfying (4), namely* $\sigma = x\,H(m_n)$.

Proof. By bilinearity $e(H(m_n), x g_2) = e(xH(m_n), g_2)$, so (4) gives $e(\sigma - xH(m_n),\; g_2) = 1$. Since $e(\cdot, g_2)$ is non-degenerate on the cyclic group $\mathbb{G}_1$ of prime order, its kernel is trivial and $\sigma = xH(m_n)$. $\square$

Lemma 2 is the reason settlement can be permissionless: whoever submits the signature, the outcome is the same, and there is nothing to grind. Unpredictability rests on the standard threshold assumption that fewer than t drand nodes collude, together with the hardness of computing $xH(m)$ without x (co-CDH on BN254).

4.2 From signature to cell

The contract derives

$$\begin{aligned} \rho_r &= \mathrm{SHA256}(\sigma_{n_r}) \in \{0, \dots, 2^{256} - 1\}, \\ w_r &= \rho_r \bmod 25, \qquad J_r = \mathbf{1}\big[\,\mathrm{keccak256}(\rho_r) \bmod 625 = 0\,\big]. \end{aligned} \tag{5}$$

Cell k is labelled by column $\texttt{abcde}[k \bbmod 5]$ and row $5 - \lfloor k/5 \rfloor$, so $k = 12$ is `c3`.

Proposition 3 (modulo bias). *Let* $N = 2^{256}$ *and assume* ρ_r *is uniform on* $\{0, \dots, N-1\}$. *Since* $N = 25Q + 11$ *with* $Q = \lfloor N/25 \rfloor$,

$$\Pr[w_r = k] = \frac{Q + \mathbf{1}[k < 11]}{N}, \qquad \Big|\Pr[w_r = k] - \tfrac{1}{25}\Big| \le \frac{14}{25N}, \tag{6}$$

and the total variation distance from the uniform distribution on 25 *cells is*

$$\delta_{\mathrm{TV}} = \frac{1}{2} \sum_{k=0}^{24} \Big|\Pr[w_r = k] - \tfrac{1}{25}\Big| = \frac{11 \cdot 14}{25 \cdot 2^{256}} \approx 5.3 \times 10^{-77}. \tag{7}$$

For the jackpot, $N = 625Q' + 561$ *and* $\Pr[J_r = 1] = \frac{1}{625} + \frac{64}{625N}$.

Proof. Residues $0, \dots, 10$ occur $Q + 1$ times and residues $11, \dots, 24$ occur Q times among $0, \dots, N-1$. Then $\frac{Q+1}{N} - \frac{1}{25} = \frac{25 - 11}{25N}$ and $\frac{Q}{N} - \frac{1}{25} = -\frac{11}{25N}$; summing the eleven positive and fourteen negative deviations gives (7). The same count with 625 and remainder 561 gives the jackpot probability. $\square$

Modelling SHA-256 and keccak-256 as random oracles, ρ_r is uniform given σ_{n_r} and the pair (w_r, J_r) is independent up to the same negligible terms, so $\Pr[w_r = k,\ J_r = 1] = \frac{1}{15\,625} + O(2^{-256})$.

4.3 Settlement and liveness

`settle(r, σ)` can be called by anyone at any time $t \in [c_r,\ c_r + \Delta)$ for a round with $T > 0$. A keeper bot calls it a few seconds after each close; in local tests settlement lands 3–5 s after c_r at a cost of about 2.5×10^5 gas, including the pairing check.

Proposition 4 (no outcome control). *No party can change w_r or J_r. A party can only refrain from settling; if every party refrains until $c_r + \Delta$, each player recovers u_i in full and no fee is charged.*

Proof. By Lemma 1 the beacon is unknown while bets are open; by Lemma 2 the only accepted input is the unique signature, and (5) is a deterministic function of it. Settlement after $c_r + \Delta$ reverts, while `refund(r)` pays u_i from that moment. □

Withholding is not a profitable veto: the beacon is public within seconds of the close, and every winner of the round has an incentive to submit it.

5 Payouts

Fix a settled round and drop the index r. Let w be the winning cell and $L = T - S_w$ the losing stake. All divisions are integer divisions on wei, written $\lfloor \cdot \rfloor$.

5.1 Settled round with players on the winning cell ($S_w > 0$)

$$F = \lfloor \varphi L \rfloor, \qquad \Pi = L - F, \qquad x_i = s_{i,w} + \left\lfloor \frac{\Pi\, s_{i,w}}{S_w} \right\rfloor, \qquad y_i = \left\lfloor \frac{E\, s_{i,w}}{S_w} \right\rfloor, \tag{8}$$

where x_i is the HYPE paid to player i, y_i the LAUREL minted to them, and the token pool is

$$E = e + J \cdot \mathcal{M}, \qquad \mathcal{M} \leftarrow \begin{cases} 0 & \text{if } J = 1, \\ \mathcal{M} & \text{otherwise.} \end{cases} \tag{9}$$

A winner thus receives the stake on the winning cell back plus the gross odds $1 + (1-\varphi)L/S_w$ on it; the fee is charged only on losing stake.

5.2 Void round ($S_w = 0$)

$$F = \lfloor \varphi T \rfloor, \qquad x_i = \left\lfloor \frac{(T - F)\, u_i}{T} \right\rfloor, \qquad y_i = 0, \qquad \mathcal{M} \leftarrow \mathcal{M} + e, \qquad J := 0. \tag{10}$$

5.3 Jackpot accrual

Every settled round adds j to the jackpot before the payout, so a round that triggers $J = 1$ pays the accrual of its own round as well:

$$\mathcal{M}_r = \mathcal{M}^{+}_{r-1} + j, \qquad \mathcal{M}^{+}_r = \begin{cases} 0 & S_{w_r} > 0,\ J_r = 1, \\ \mathcal{M}_r + e & S_{w_r} = 0, \\ \mathcal{M}_r & \text{otherwise.} \end{cases} \tag{11}$$

Lemma 5 (conservation). *For every settled round, $\sum_i x_i + F \le T$, and the undistributed remainder $T - F - \sum_i x_i$ is smaller than the number of winners, in wei. An unsettled round pays exactly $\sum_i u_i = T$ through refunds.*

Proof. In case (8) let $n_w = |\{i : s_{i,w} > 0\}|$. Then $\sum_i s_{i,w} = S_w$ and $\sum_i \lfloor \Pi s_{i,w}/S_w \rfloor \in (\Pi - n_w,\ \Pi]$, so $\sum_i x_i \in (S_w + \Pi - n_w,\ S_w + \Pi]$ with $S_w + \Pi + F = T$. Case (10) is identical with u_i and T in place of $s_{i,w}$ and S_w. □

The owner can withdraw only the booked fees $\sum_r F_r$, so the contract's HYPE balance always covers every outstanding claim and refund.

6 Expected value

Treat the book $\{s_{i,k}\}$ of a round as fixed at the close and ignore wei rounding. Conditioning on the uniform winning cell gives the exact expectation of a player's HYPE return.

Proposition 6 (expected return).

$$\mathbb{E}[x_i] \;=\; \frac{1}{25}\left[\sum_{k\in K^+} s_{i,k}\left(1 + (1-\varphi)\,\frac{T - S_k}{S_k}\right) \;+\; |K^0|\,(1-\varphi)\,u_i\right]. \tag{12}$$

Proof. If $w = k \in K^+$, (8) pays $s_{i,k}(1 + \Pi/S_k)$ with $\Pi = (1-\varphi)(T - S_k)$. If $w \in K^0$, (10) pays $(1-\varphi)u_i$. Each cell wins with probability $1/25$ by Proposition 3. □

Corollary 7 (the fee does not depend on the book). *For every distribution of stakes,*

$$\mathbb{E}[F] \;=\; \frac{24}{25}\,\varphi\,T, \qquad \mathbb{E}\Big[\sum_i x_i\Big] \;=\; T\left(1 - \frac{24\varphi}{25}\right). \tag{13}$$

At $\varphi = 0.10$ the expected take is 9.6% of the round.

Proof. $\mathbb{E}[F] = \frac{\varphi}{25}\big[\sum_{k\in K^+}(T - S_k) + |K^0|\,T\big] = \frac{\varphi}{25}\big(|K^+|T - T + |K^0|T\big) = \frac{24}{25}\varphi T$, using $\sum_{k\in K^+} S_k = T$ and $|K^+| + |K^0| = 25$. The second identity follows from Lemma 5. □

Corollary 8 (uniform book). *If $S_k = T/25$ for all k, every player has $\mathbb{E}[x_i] = u_i\,\big(1 - \frac{24\varphi}{25}\big)$, whatever their own split across cells.*

6.1 Where a marginal bet pays

Differentiating (12) for a new stake $\delta \to 0$ on a covered cell k gives its expected return per unit of stake:

$$R_k \;=\; \frac{1}{25}\left[1 + (1-\varphi)\,\frac{T - S_k}{S_k} + |K^0|\,(1-\varphi)\right]. \tag{14}$$

With every cell covered ($K^0 = \varnothing$), a bet on k has positive expected HYPE return exactly when

$$R_k > 1 \iff \frac{S_k}{T} \;<\; \frac{1-\varphi}{25-\varphi} \;\approx\; 3.614\% \quad (\varphi = 0.10), \tag{15}$$

against the 4% share of a uniform book. The market behaves like a parimutuel: money is rewarded for going where it is scarce. Concretely, if player A stakes 0.1 on all 25 cells and player B adds 0.1 on a single cell, that cell holds 0.2 out of $T = 2.6$ (7.7%); B's expected result is -0.0528 per round (-53% of the stake), A's is -0.1968, and their sum is $-\frac{24}{25}\cdot 0.1 \cdot 2.6 = -0.2496$, as Corollary 7 requires.

Proposition 9 (empty cells do not stay empty). *A stake δ on an empty cell has expected profit*

$$\mathbb{E}[\text{profit}] \;=\; \frac{(1-\varphi)\,T}{25} \;-\; \delta\left(1 - \frac{1 + (|K^0|-1)(1-\varphi)}{25}\right), \tag{16}$$

where T is the book before the bet. It is strictly positive for every $\delta < \dfrac{(1-\varphi)T}{24 - (|K^0|-1)(1-\varphi)}$.

Proof. If the cell wins (probability $1/25$) the bettor is alone on it and receives $\delta + (1-\varphi)T$; if another empty cell wins the round is void and returns $(1-\varphi)\delta$; otherwise the stake is lost. □

In an active market every cell is covered at the minimum stake or more, void rounds disappear, and the emission is always paid to someone.

6.2 Risk of a single position

A stake s on one covered cell pays $s\,o_k$ with probability $1/25$, where $o_k = 1 + (1-\varphi)(T - S_k)/S_k$, and nothing otherwise (no empty cells). Its variance is

$$\operatorname{Var}[x] \;=\; s^2\,o_k^2 \cdot \frac{1}{25} \cdot \frac{24}{25}, \tag{17}$$

By contrast, in a uniform book a position spread evenly over all 25 cells returns $u_i\big(1 - \frac{24\varphi}{25}\big)$ whichever cell wins: its HYPE variance is zero, and the holder is exposed only to the fee and to the value of the tokens it mines.

7 Mining economics

LAUREL enters circulation only through rounds: the emission e is split among the stakes on the winning cell, and the jackpot accrual j is paid in jackpot rounds. Covering the whole board turns the game into a mining process: the miner gives up the expected fee and receives a share of every round's emission.

Proposition 10 (free-entry equilibrium). *Let n identical miners each stake b on every cell, with no other bettors, and let π be the market price of LAUREL in HYPE. Each miner bears an expected HYPE cost $24\varphi b$ per round and receives $(e+j)/n$ LAUREL per round in the long run. If miners enter until expected profit is zero,*

$$n \cdot 24\,\varphi\,b \;=\; \pi\,(e + j), \tag{18}$$

i.e. the fees paid to the protocol equal the market value of the tokens mined.

Proof. Each miner holds the same share $1/n$ of every cell, so it receives $1/n$ of each round's pool and of each jackpot. By Corollary 8 its expected HYPE loss is $25b \cdot \frac{24\varphi}{25} = 24\varphi b$. Zero profit is $\pi(e+j)/n = 24\varphi b$. □

This is the same rent-dissipation logic as proof-of-work: competition for the emission raises the cost of mining until it matches the value of what is mined. The marginal cost of one LAUREL is $24\varphi b\,n/(e+j)$ HYPE, which ties the protocol's fee revenue to the token's market price.

7.1 Jackpot

In a fully covered market the jackpot fires in each settled round independently with probability $q = 1/625$. The number of rounds G between two jackpots is geometric:

$$\Pr[G=g]=(1-q)^{g-1}q, \qquad \mathbb{E}[G]=\frac{1}{q}=625, \qquad \sqrt{\mathrm{Var}[G]}=\frac{\sqrt{1-q}}{q}\approx 624.5, \tag{19}$$

so a jackpot is paid on average every $625\cdot P\approx 13.0$ hours, and its size $\mathcal{M}=jG$ has $\mathbb{E}[\mathcal{M}]=625\,j$ with a standard deviation of about $624.5\,j$. Void rounds add e each, which is why uncovered boards grow the jackpot faster.

7.2 Supply

LAUREL is an ERC-20 with a hard cap $M_{\max}=3\,000\,000$, minted only by the game contract and clipped at the cap. There is no premine. Every settled round allocates $e=1$ to the winners and $j=0.2$ to the jackpot, and accrues to the treasury a share $\tau=10\%$ of all LAUREL created, $a=(e+j)\,\tau/(1-\tau)\approx 0.133$, which anyone can mint to the treasury address. Issuance is bounded by

$$\frac{\mathrm{d}\,\mathrm{Supply}}{\mathrm{d}t}\;\le\;\frac{86\,400}{P}\cdot\frac{e+j}{1-\tau}=1536\ \text{per day}, \qquad t_{\mathrm{cap}}\;\ge\;\frac{M_{\max}(1-\tau)}{1152\,(e+j)}\approx 5.35\ \text{years}. \tag{20}$$

Fees are paid in HYPE and split equally: half buys LAUREL on the market and burns it, half funds the treasury (keeper gas, audits, liquidity, development). Buybacks happen outside the game contract and are published on-chain.

8 Administration

Owner can	Owner cannot
set the fee for future rounds, $\varphi\le 15\%$	change the fee of a round that already has bets
pause new bets	block settlement, claims or refunds
withdraw booked fees $\sum_r F_r$	move players' stakes or winnings
change the treasury address	mint LAUREL beyond the treasury's 10%
transfer ownership in two steps	change timing, randomness source, emission, cap or minimum stake

Timing (t_0,P,W), the randomness verifier, the token, e, j, $M_{\max}$ and $s_{\min}$ are immutable.

9 Assumptions and risks

- **drand.** Unpredictability assumes fewer than t of the N beacon nodes collude. A beacon outage leads to full refunds after Δ.
- **Sequencer.** Elysium is an Arbitrum Orbit chain with a single sequencer that orders transactions and sets block timestamps within protocol bounds. A sequencer that stalls block production past c_r, observes the beacon and then inserts a bet with an earlier timestamp could bias its own result. LAUREL assumes an honest sequencer, as does every time-based application on the chain.
- **Implementation.** The pairing check uses the open-source `bls-solidity` library, which has not been audited; the game contract has not been audited yet. An audit is planned before mainnet.
- **Keeper.** Settlement is permissionless; if the keeper fails, anyone can settle with the public beacon, and refunds open after Δ.

- **Token value.** Proposition 10 describes an equilibrium; the market price of LAUREL is not guaranteed and can fall below the cost of mining it.

Appendix A Parameters

Constant	Value	Note
`CELLS`	25	5×5 grid
`roundDuration`, `betWindow`	75 s, 60 s	break of 15 s
`MAX_FEE_BPS`	1500	$\varphi \le 0.15$; default 1000
`MOTHERLODE_ODDS`	625	jackpot probability $1/625$
`REFUND_DELAY`	3600 s	Δ
`DRAND_GENESIS`, `DRAND_PERIOD`	1 727 521 075, 3 s	drand evmnet
`emissionPerRound`, `motherlodePerRound`	1, 0.2 LAUREL	e, j
`treasuryBps`	1000	treasury share $\tau = 10\%$
`maxSupply`	3 000 000	$M_{\max}$

Appendix B Settlement

```
settle(r, σ):
    require not settled[r]
    require c_r ≤ now < c_r + Δ and T_r > 0
    ρ  ← SHA256(σ)  after  e(σ, g₂) = e(H(keccak256(be64(n_r))), PK)   // reverts otherwise
    w  ← ρ mod 25
    J  ← (keccak256(ρ) mod 625 = 0)
    M  ← M + j
    if S_w = 0:                         // void round
        F ← ⌊ϕ·T⌋;  pot ← T − F;  M ← M + e;  J ← false
    else:
        F ← ⌊ϕ·(T − S_w)⌋;  pot ← T − S_w − F
        E ← e;  if J: E ← E + M;  M ← 0
    fees ← fees + F
    emit Settled(r, w, J, pot, E, F)
```

This document describes the contracts as of version 0.1. Figures marked as deployment parameters will be published together with the contract addresses. Nothing here is an offer of securities or a promise of returns.