OFFICIAL TECHNICAL WHITEPAPER

Project Whitepaper: Provably Fair Web3 Competitive Gaming

A Zero-Trust PvP Ecosystem Built on Deterministic Cryptography & Fair-Launch Tokenomics

Protocol: WAGMINE **Token:** $WAGMI (ERC-20) **Version:** 1.1 (Production) **Published:** 2026

1. Abstract & Vision

In the traditional Web2 gaming industry, players operate in a "black box" environment. Server-side Random Number Generation (RNG), matchmaking algorithms, and economic variables are completely hidden, requiring players to blindly trust operators. Furthermore, the economic value generated by competitive players is entirely extracted by centralized game studios.

WAGMINE introduces a decentralized, zero-trust competitive gaming ecosystem built around the classic logic game, **Minesweeper Flags**. By combining a high-performance Web2.5 architecture with cryptographic commitment schemes, Merkle Tree batching, and on-chain anchoring, we provide mathematical guarantees of fairness while delivering instantaneous, gas-free gameplay.

The ecosystem is powered by the **$WAGMI** token, an ERC-20 utility and reward asset governed by a strict **100% Fair Launch** model with zero premine, zero private sales, and zero team allocations. Economic sustainability is enforced via triple-deflationary burn mechanisms, while our proprietary Trust Engine provides robust Sybil resistance and automated anti-cheat protection.

2. Game Mechanics & Matchmaking

2.1 The Rules of Flag Hunting

Unlike traditional survival-based Minesweeper where clicking a mine ends the run, WAGMINE Flag Hunting is a zero-sum, turn-based PvP game of tactical area control and logical deduction.

- **The Grid:** Standard competitive matches take place on a standardised 16×16 grid containing exactly 40 hidden flags (mines). Custom and tiered modes support varying board dimensions.
- **Turn Mechanics:** Players alternate turns clicking concealed tiles. If a player clicks a safe tile, it reveals an adjacent flag counter (0–8) and their turn concludes. If a player successfully reveals a flag tile, they capture it for +1 point and *maintain their turn*, enabling skilled players to chain complex deductions consecutively.
- **Win Condition:** The match ends as soon as a player captures the majority of flags (21 out of 40) or when all 40 flags have been uncovered. The player with the highest flag count wins.
- **Clocks & Forfeits:** Strict per-turn timers prevent stalling. Exceeding the turn timer automatically passes the turn; complete disconnection or intentional resignation records a decisive forfeit loss.

2.2 Elo Rating System

Matchmaking and seasonal rankings are governed by a modified Elo algorithm to ensure competitive integrity. A player's expected score (E_A) against opponent B is computed dynamically based on their respective MMR ratings:

```
E_A = 1 / (1 + 10^((R_B - R_A) / 400))
R_A' = R_A + round(K * (S_A - E_A))
```

Where S_A represents the outcome (1.0 for a win, 0.0 for a loss, 0.5 for a draw), and K is the rating volatility factor (standard K=32). Ratings are clamped strictly within the range [0, 10,000], with new accounts initialized at 1,000 MMR.

In addition to MMR adjustments, matches award **Leaderboard Points (LP)**. LP rewards scale dynamically based on match outcome, opponent skill disparity, and the player's verified Trust Score multiplier, accumulating throughout the weekly season toward reward distribution.

3. Cryptographic Fairness Engine (Zero-Trust Architecture)

To mathematically prove that the server does not manipulate board generation or peek at mine positions during gameplay, WAGMINE implements a strict **Cryptographic Commitment Scheme** combined with periodic on-chain Merkle anchoring.

3.1 Pre-Game Hash Commitment

1. **Generation:** Before match start, the game server generates a cryptographically secure pseudo-random seed and secret salt that deterministically constructs the full board layout.
2. **Commitment:** The server computes the canonical SHA-256 hash of the complete board layout combined with the secret salt.
3. **Locking:** This commitment hash is transmitted to both player clients inside the initial match handshake before any player makes a move. The server is mathematically locked into this exact layout.
4. **Verification:** Upon match completion, the server reveals the raw secret salt. The client-side Verification Drawer independently regenerates the board and recomputes the hash to confirm it matches the pre-game commitment.

3.2 On-Chain Merkle Anchoring

Writing every move or individual match to the blockchain introduces latency and unsustainable gas costs. Instead, WAGMINE utilizes an asynchronous **Merkle Batching Engine**.

Completed match results are packaged into canonical leaf hashes:

```
leafHash = keccak256(abi.encode(matchId, player1, player2, winnerId, score1, score2,
boardHash, timestamp, salt))
```

Batches are compiled into a cryptographic Merkle tree, and the resulting Merkle Root is anchored to public smart contracts. Any player can request their lightweight cryptographic Merkle Proof to

independently verify their match outcome against the on-chain root using standard cryptographic libraries or our Verification Drawer.

4. Tokenomics & $WAGMI Utility

The **$WAGMI** token is an ERC-20 utility and reward token designed with strict deflationary sink-and-source mechanics, programmatic seasonal emissions, and a radically player-centric distribution model.

4.1 Token Allocation & Supply

In a stark departure from predatory Web3 gaming models, WAGMINE implements a strict **100% Fair Launch**. There are zero venture capital allocations, zero private presales, zero advisor pools, and zero team unlocks. The token contract launches at a total supply of exactly zero.

- **Maximum Supply:** 10,000,000,000 $WAGMI (10 Billion Cap)
- **Zero Premine:** 0% allocated at genesis; every token in circulation is minted programmatically by `EmissionManager.sol`.
- **100% Gameplay Distribution:** The entire supply is distributed exclusively through competitive gameplay rewards, seasonal leaderboard prize pools, and tournament structures.
- **Proof of Skill:** The only mechanism to introduce $WAGMI into circulation is competing in the arena and proving legitimate skill.

4.2 Utility & Sinks

- **Tournament Entry:** High-stakes competitive tournaments and special bracket events require a $WAGMI entry fee.
- **Cosmetic Armory & Marketplace:** Players can spend $WAGMI in the Armory to acquire exclusive ERC-1155 avatar items, board skins, animated cursors, and profile badges.
- **Gasless Claims & Off-Chain Ledger:** Gameplay earnings are tracked in an off-chain ledger for instant zero-gas updates. On-chain claims are routed gaslessly via backend relayers from `RewardTreasury.sol`.

4.3 Algorithmic Distributions

Tokens are emitted on a strict weekly season lattice managed by `EmissionManager.sol`. At the conclusion of each one-week season, the seasonal pot is distributed pro-rata among all eligible players based on Leaderboard Points (LP):

```
Player Reward = (Player Seasonal LP / Total Eligible Seasonal LP) * Season Emission Amount
```

To prevent retroactive supply inflation after unexpected outages, seasons feature a strict **72-Hour Finalization Window**. If an emission is not allocated within 72 hours of season close, the allocation is permanently forfeited and burned.

4.4 Deflationary Burn Mechanics

WAGMINE enforces triple-deflationary token sinks where tokens are permanently transferred to the standard dead address (`0x000000000000000000000000000000000000dEaD`):

- **100% Store Purchase Burns:** All $WAGMI spent in the cosmetic store is permanently burned. The platform accumulates zero corporate treasury float.
- **Trust-Tier Withdrawal Tax Burns:** Any withdrawal penalty fees incurred by low-to-moderate trust accounts are permanently burned rather than retained by the house.
- **Expired Guest Forfeiture Burns:** Unclaimed balances of abandoned or deleted guest accounts past the 90-day retention grace period are atomically burned.

4.5 Multi-Game Ecosystem & Game Registry

Through the `GameRegistry.sol` smart contract, the WAGMINE platform supports modular on-chain registration of new competitive skill-based games. The protocol owner can allocate emission weights (up to 10,000 basis points total) across approved game modules, establishing $WAGMI as a universal cross-game reward currency.

5. Sybil Resistance & The Trust Engine

Web3 gaming economies are frequently destroyed by automated bot farms and Sybil attackers. WAGMINE eliminates this risk through an intelligent, multi-layered **Trust Score (0 to 100 / 0.0 to 1.0)**, evaluated asynchronously after every match.

5.1 Multi-Signal Anti-Cheat Telemetry

- **On-Chain Identity Footprint:** Linking a verified Web3 wallet with established transaction history and age (>90 days) grants the `isVerifiedHuman` shield and significant Trust Score boosts.
- **Behavioral Telemetry Analysis:** The engine inspects inter-click timing deltas (flagging sub-50ms mechanical clicks), mouse trajectory smoothness, and keyboard input cadences to distinguish humans from scripts.
- **Social Verification:** Connecting multi-factor identity providers (Discord, Twitter, Google) increases initial trust baselines.

5.2 Trust Brackets & Withdrawal Taxes

TRUST SCORE	TIER	WITHDRAWAL TAX	ECOSYSTEM STATUS
90 – 100	**Excellent**	0% (Full Payout)	1.0x LP Multiplier, Instant Gasless Claims
70 – 89	**Good**	5% (Burned)	Standard LP Multiplier, Normal Processing
50 – 69	**Fair**	15% (Burned)	Moderate Friction, Elevated Telemetry Monitoring
25 – 49	**Low**	35% (Burned)	Heavy Economic Friction, Reduced Matchmaking Priority
0 – 24	**Restricted**	**Blocked**	Withdrawals Disabled, Excluded from Seasonal Prize Pools

6. Development Roadmap

Phase 1 — Now **Core Platform & Community (Completed):** Real-time WebSocket PvP engine, provably fair seeded board generation, on-chain Merkle anchoring of match results, public replay & verification drawer per game, live public leaderboard & ranked Elo ladder, anti-abuse Trust Engine, and official whitepaper publication.

Phase 2 — Q3 2026 **Chain Selection & Security Audit (In Progress):** Selecting optimal low-cost L2 home chain for launch, comprehensive $WAGMI smart contract security audits, and public testnet deployment for community testing & feedback.

Phase 3 — Q4 2026 **Mainnet Launch & Token Emission (Upcoming):** Production mainnet deployment on selected chain, zero-supply 100% fair launch (no presale, no allowlist), weekly season emissions live, on-chain Merkle root match locking, in-game $WAGMI fee payments & cosmetic store burns, and post-launch liquidity pool setup.

Phase 4 — Q1 2027 **Growth & Mobile PWA (Upcoming):** Exclusive seasonal competitive tournaments with dedicated prize pools, and mobile-responsive Progressive Web App (PWA) for iOS and Android browser gaming.

Phase 5 — Q2–Q3 2027 **Native Mobile Apps & Platform Growth (Upcoming):** Native iOS & Android app store releases, cross-game cosmetics & Armory ecosystem fully live, and seasonal sponsorships & Web3 co-marketing partnerships.

Phase 6 — Q4 2027 **Game #2 — Provably Fair Poker (Upcoming):** Poker alpha on testnet powered by the unified $WAGMI token and player accounts, poker mainnet launch with cryptographic card shuffling & on-chain proofs, and shared cosmetics & cross-game avatars active across both titles.

7. Smart Contract Architecture & Security

7.1 Smart Contract Architecture

All smart contracts are written in Solidity (0.8.28), audited, and built on OpenZeppelin standards:

- `WagmiToken.sol`: ERC-20 token with EIP-2612 permit capabilities, fixed 10B cap, and zero premine.
- `EmissionManager.sol`: Enforces fixed weekly emissions on a strict lattice with a 72-hour forfeiture window.
- `RewardTreasury.sol`: Manages reward reserves with per-tx caps (100k WAGMI) and 24h rolling leaky-bucket limits (1M WAGMI).
- `FeeCollector.sol`: Manages native chain fee collection for gasless transaction execution.

- `GameRegistry.sol`: Dynamic multi-game registry managing emission weight allocations across gaming titles.
- `WagmineArmory.sol`: ERC-1155 cosmetic item armory supporting ERC-2981 royalties and soulbound achievements.

7.2 Access Control & Guardian Model

Security is built on a 3-tier operational hierarchy:

- **Owner (Cold Administration):** Governed by a multi-signature Safe protected by a 2-day TimelockController for high-impact protocol configurations and parameter updates via `Ownable2Step`.
- **Guardian (Warm Emergency Brake):** Fast-response emergency keys capable of triggering `pause()` without holding any fund-movement or withdrawal capabilities.
- **Emission Operator (Hot Routine Key):** Automated worker key strictly limited to scheduled weekly season finalization and minting into pre-approved contracts.

All protocol parameters, emission allocations, and contract configurations are strictly controlled via multi-sig authorization and timelock delays to ensure complete security and operational predictability.

8. Legal Disclaimers

> *The $WAGMI token is strictly a digital utility token intended solely for use within the WAGMINE gaming ecosystem. It is not an investment contract, security, or financial instrument. Acquisition or holding of $WAGMI carries no rights to company dividends, equity ownership, or guaranteed economic returns.*
>
> *WAGMINE is a skill-based competitive logic game. Participation in tournaments and gameplay distributions is subject to applicable local laws and regulations. Users are responsible for ensuring compliance with the legal frameworks in their respective jurisdictions.*