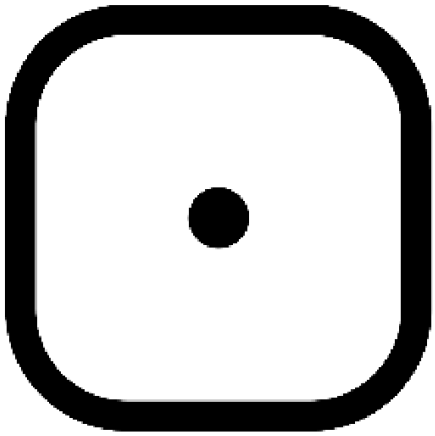

HEMIS

Simple tools for popular games.

Non-Technical White Paper

Version 3.0 – May 2026
Vileda, Core Team

Version 2.0 – July 2023

Daniel Ames, Project Co-Founder

Dedicated to Takosha Churu (1981 - 2023)

Veteran developer, colleague, and friend. Hugely missed.

Contents

What is Hemis?

Hemis is a Layer 1 blockchain platform purpose-built for verifiable randomness in games. It gives game developers a simple API to request random outputs - dice rolls, card draws, player selections. Each result is generated and signed by a decentralised network of Gamemaster nodes.

The design separates two concerns that most platforms conflate: randomness generation and on-chain commitment. Randomness generation happens in memory across the Gamemaster quorum and completes in 1-3 seconds. On-chain commitment follows automatically in the background and serves as the permanent verifiable record. Games do not wait for it.

No smart contracts. No Solidity. No deep blockchain knowledge required. If you can make an API call, you can build a provably fair game on Hemis.

The Problem with Digital Dice

Anyone who has played competitive games online knows the feeling: the result does not feel fair, but you cannot prove it. Game publishers and platform hosts control the randomness engine, and players have no way to verify it has not been manipulated.

Blockchain was supposed to fix this. In practice, building provably fair games on existing chains means writing expensive smart contracts and managing complex infrastructure. It also requires your players to understand cryptography before they can trust the outcome. The result: most developers give up before they start.

True randomness is surprisingly difficult to achieve. Programming randomness is easy in principle but very hard in practice for machines designed to follow logical rules. Competition gamers will not use digital dice when the result really matters. Professional gamblers still prefer not to play online. This problem is real, it is large, and it has not been solved.

Hemis is built differently.

The Hemis Opportunity

Dice-based games and games of chance have an enduring history spanning thousands of years and every culture on earth. Their appeal is simple: low barriers to entry, immediate participation, and the genuine unpredictability of the outcome. Hemis aims to capture that appeal and reproduce it in a simple digital toolkit.

The global market for online gaming and gambling is enormous and continues to grow. The demand for provably fair outcomes is increasing as players become more sophisticated. Regulatory environments in many jurisdictions are moving toward requiring demonstrable fairness. Hemis is positioned to serve this demand with technology that was previously unavailable.

The Hemis opportunity is not to compete with complex blockchain gaming projects. It is to solve a specific problem very well: give any developer, anywhere, the ability to build games with outcomes that are

genuinely and demonstrably fair. Delivered quickly, without needing to understand the underlying cryptography.

How Hemis Works

The Simple Version

A game server calls the Hemis API. It specifies what it needs: roll 2 six-sided dice, draw 5 cards from a 52-card deck, select a player from a pool of 50. Hemis returns a result in 1-3 seconds. The result is signed by a network of independent Gamemaster nodes. No single party - including Hemis - could have predicted or influenced the outcome. The proof is permanently recorded on the blockchain and can be verified by anyone at any time.

The Randomness Engine

Each Hemis random result is produced by a quorum of Gamemaster nodes using threshold BLS cryptography. BLS (Boneh-Lynn-Shacham) signatures have a property that makes them uniquely suited to randomness generation: for any given input and quorum public key, there is exactly one valid output. It is mathematically impossible for any combination of nodes below the threshold to produce a different result, or to predict the result in advance.

This is not deterrence - it is a mathematical property. A Gamemaster node that wants to bias a result has no mechanism to do so. Its only options are to contribute its partial signature, producing the correct result, or to abstain. Abstaining changes nothing: the remaining honest nodes reach the threshold without it.

Why Results Arrive in 1-3 Seconds

Most blockchain randomness systems make players wait for block confirmations - often several minutes. Hemis solves this by separating result delivery from on-chain commitment entirely.

When a game calls the API, the assigned Gamemaster quorum signs the result immediately in memory. Partial signatures propagate across the quorum via peer-to-peer gossip. Once the threshold is reached, the full signature is reconstructed and the result returned to the caller. This typically completes in 1-3 seconds. The on-chain proof follows automatically in the background when the caller accepts the result.

This is the same signing path the Hemis network already uses for ChainLocks - sub-second threshold signing is live infrastructure, not a new dependency.

Round Seed Construction

Every PTX round uses a unique seed constructed from five inputs: the game ID, the current block height, the caller's public key, a nonce, and the output parameters. These are hashed together in memory at call time with no block wait.

Block height inclusion is critical. It anchors the round to a specific point in time and prevents result grinding: a caller cannot obtain a different result by re-calling within the same block, because the seed is identical across calls at the same height. The caller must wait approximately 60 seconds for a genuinely different seed.

The nonce is constructed from the previous round's quorum output combined with a caller-provided salt. This means no caller can pre-compute the nonce offline to search for favourable seeds - the quorum-produced component is unknown until the prior round completes.

What Happens to the Result

The raw beacon output - a 256-bit number - is mapped to game values using mathematically correct techniques. Dice rolls and range selections use rejection sampling to eliminate the modulo bias that naive implementations introduce. Unique draws (card hands, player selections) use a Fisher-Yates shuffle seeded from the beacon output, guaranteeing uniform distribution with no repeated values.

The on-chain record contains only the numeric result and parameters. The caller maps numeric outputs to game-layer meaning (card names, player identities). This keeps the protocol clean and generic.

Gamemaster Nodes

What They Do

Gamemaster nodes are the network's randomness engine. Each node participates in assigned quorums, contributes a partial BLS signature to each round, and propagates signatures to other quorum members. The quorum collectively produces the beacon output without any single node being able to see or influence the final result.

Gamemasters are also responsible for the daily lottery that distributes transaction fee rewards across honest participants. Any node operator can participate by staking the required collateral.

How Bad Actors Are Prevented

Defence operates at two distinct levels. Each is independent - failure of one does not compromise the other.

Level 1 - Cryptographic (cannot be circumvented): Threshold BLS signatures are deterministic. For a given round seed and quorum public key, there is exactly one valid output. A Gamemaster node cannot choose between outputs. It can only sign or abstain. Abstaining does not bias the result. Manipulation at the signing layer is not economically deterred - it is mathematically impossible.

Level 2 - Incentive design (removes the motive): Gamemaster rewards from transaction fees are distributed through a daily lottery across all nodes that participated honestly in the preceding 24-hour window. Each honest round participation earns one lottery ticket. Non-participation results in PoSe score accumulation and lottery ticket forfeiture. No Gamemaster can predict whether any specific round will generate a reward, eliminating the financial incentive to target individual rounds.

A third potential defence layer - collateral slashing - was evaluated and explicitly rejected. The cryptography already makes output manipulation impossible. The lottery already handles participation incentives. Introducing slashable capital positions creates new attack surface: a competitor could deliberately trigger penalty conditions against honest nodes to eject them from the network and weaken the quorum pool. Complexity that introduces real attack surface without mitigating a real problem is not added to Hemis.

Collateral and Registration

Every Gamemaster node stakes 1,000 HMS coins as operational collateral to register on the network. This collateral is a Sybil-resistance mechanism - it raises the cost of registering many nodes to statistically dominate quorum selection. It is held in a separate protocol-level pool from any participation mechanism and cannot be forfeited by any penalty mechanism. A node can only lose its operational collateral by voluntarily deregistering.

The thin liquidity of HMS on current markets provides additional Sybil resistance beyond the nominal collateral figure. Acquiring enough HMS to register 33% of the network would move the price significantly during accumulation and be visible on-chain before any attack could be completed.

Quorum Design

Gamemaster quorums are drawn deterministically from the active node pool. Every observer reproduces the same member list from on-chain data alone, with no leader election or interactive randomness. Quorum selection uses the previous round's recovered threshold signature as its entropy input, preventing miners from grinding block hashes to influence which Gamemasters are assigned to high-value rounds.

Quorum size is staged as the network matures. Testnet begins with 5-11 nodes. Mainnet targets 21+ nodes with a threshold of approximately 67%. Increasing quorum size does not increase latency to the caller - the result is returned once the threshold is reached regardless of total quorum size.

For Game Developers

Hemis removes the hard parts of building fair games. A single API call returns everything needed to resolve a game action and prove the result was fair.

- No contract writing. The randomness logic lives in the Hemis protocol. You call an API, you get a result.
- Platform agnostic. Build on web, mobile, desktop, or any game engine. Hemis connects via a standard RPC API.
- Flexible outputs. Request dice rolls, unique card draws, player selections, or any combination. You define the range and count.
- Fast. Results in 1-3 seconds. Suitable for real-time gameplay.
- Auditable. Every result is anchored to the blockchain. Players can independently verify fairness at any time.

The API is intentionally simple. A game server specifies mode (dice, cards, players), count, range, and whether draws should be unique. The response includes the drawn values, the round seed for verification, the quorum signature as cryptographic proof, and the block height at call time.

A node operator runs a Hemis P2P node to connect their game to the network. No other infrastructure is required.

Project History

In 2014, Hemis co-founders Daniel and Fabian helped build the first blockchain layer-2 service layer at Dash. Dash was the first project with a second-tier node network delivering instant confirmation and private transactions via a masternode quorum. That work prompted Daniel to consider how deterministic quorum subsets of peer-to-peer networks could address one of computing's oldest unsolved problems: generating genuinely random numbers.

In the years that followed, Daniel and Fabian explored various applications of quorum-based systems. In 2019, Daniel identified provably fair decentralised randomness - without needing to write smart contracts - as the most powerful and accessible application of the technology. In early 2020, a group of gaming enthusiasts, technologists, blockchain developers and software engineers convened to assess the opportunity. The conclusion was clear: low technical barriers to entry combined with provably fair outcomes could gain significant adoption.

In 2021, the group was joined and led by veteran blockchain developer Takosha Churu, who created the first live blockchain showcasing probabilistic transactions. The prototype was a success, but it revealed that certain design choices - particularly the use of miniscript - still imposed technical barriers on game creators. A new approach was begun from the ground up.

Tragically, Takosha became unwell in early 2022 and lost his life in June 2023. He leaves behind two young children and a loving family. This project is dedicated to his memory.

The Hemis blockchain launched with a public airdrop in 2023, distributing coins broadly to ensure no single party controls the network.

Things have been quite bumpy in Hemis' journey so far, and in 2025 Daniel took a step back from the project. The Hemis community stepped up and kept things running while a new team was elected via the DAO.

Q1 of 2026 has seen renewed effort with a review of the design and purpose of Hemis. We can now confirm that PTX is now in active development, with Phase 0 validation complete and Phase 1 development in progress. As of May 2026, 410 Gamemaster nodes are active on the network.

Where We Are Now

Design Complete

The full PTX architecture has been designed, documented, and locked. Every significant decision has been recorded in a Key Design Decision register. Decisions that require real-world data to finalise - such as collateral formula calibration and fee model design - are tracked as Open Design Choices with explicit criteria for when and how they will be resolved.

The design process completed in May 2026 - ahead of the originally planned Q2 2026 target.

Phase 0 Complete

Phase 0 validated the mathematical foundation of the PTX protocol before any real node software was involved. A Python simulator implemented the full hash commit-reveal protocol state machine. It was tested against adversarial schedulers - Byzantine nodes withholding, submitting invalid commitments, abstaining. Output mapping uniformity was confirmed across all game value types. The NIST SP 800-22 statistical randomness battery was run in full.

The NIST SP 800-22 tests - the international standard for certifying random number generators - were run across 100 independent beacon streams of 2.5 million outputs each. All 15 tests passed on the official NIST reference C implementation. The beacon is statistically indistinguishable from true randomness.

Phase	Description	Status	Completion Date
Pre-Phase 0	Design Decisions & Documentation	Complete	May 2026
Phase 0	Python Protocol Simulator, NIST SP 800-22 validation	Complete	May 2026
Phase 1	Regtest, 5 nodes, real hemisd binaries, hash commit-reveal	In Progress	
Phase 2	11-node testnet, threshold BLS signing, trusted-dealer DKG	Upcoming	
Phase 3	21-node testnet, full Pedersen DKG, 16 parallel quorums	Upcoming	
Phase 4	Hybrid public testnet, external operators, real WAN latency	Upcoming	
Phase 5	Mainnet launch	Upcoming	

Technical Architecture

Layer 1 - Base Chain

A UTXO blockchain derived from Bitcoin, operating on a 60-second block time with Proof of Stake consensus. The chain stores the permanent record of every Probabilistic Transaction: the inputs, the Gamemaster quorum signatures, and the result. This is the audit layer.

Layer 2 - Gamemaster Network

A peer-to-peer network of collateralised Gamemaster nodes. These nodes generate random outputs using threshold BLS signing. No individual node can determine or influence the outcome alone. This layer already provides the same threshold signing infrastructure used for block finality today.

Cryptographic Path

Phase 1 (regtest): Hash-based commit-reveal. Each Gamemaster generates a secret, commits to it, and reveals it. The beacon is SHA256 of all revealed secrets combined. Mandatory-reveal penalties apply to nodes that commit but withhold.

Phase 2 onwards: Threshold BLS signatures using BLS12-381 via the supranational/blst library (formally verified). For any given round seed and quorum public key, there is exactly one valid output. Last-revealer advantage is eliminated entirely.

DKG approach: Phase 2 uses trusted-dealer key generation. Phase 3 upgrades to full Pedersen Distributed Key Generation - three broadcast rounds, completing in under one second. No single party ever holds the complete private key.

Chain Parameters

Chain type	UTXO, Layer 1
Base codebase	Bitcoin / PIVX
Block time	60 seconds
Consensus	Proof of Stake
Divisibility	8 decimal places
Emission	Linear over 10 years, no halving
Total supply	~30,000,000 HMS coins
Active Gamemasters	410 (as of May 2026)
Current supply	7,993,163 HMS (as of May 2026)

Coin Distribution

The Hemis project was privately funded by several investors. The launch distribution was designed to ensure that no single party has majority control over the network. All distribution is fully transparent and trackable via the official block explorer.

Category	coins	% Supply	Notes
Investors	200,000	0.67%	Distributed at launch

Category	coins	% Supply	Notes
Founders	600,000	2.00%	Distributed at launch
Airdrop	800,000	2.67%	Community distribution
Dev Fund (Year 1)	292,000	0.97%	12 monthly instalments
To be minted over 10 years	29,200,000	93.69%	Linear emission, no halving
Total supply	~30,000,000	100%	Over 10-year emission schedule

The remaining supply is minted through block rewards distributed to stakers and Gamemaster node operators over the 10-year emission schedule. There is no halving - emission is linear throughout.

A project treasurer is accountable to the community for distribution of payments to the development team and founders. All treasury addresses are published for full transparency.

Rewards and Incentives

Staking

Any holder of HMS coins can stake them to earn a share of the block reward for securing the blockchain. No special hardware is required. Staking rewards are distributed proportionally to staked balance.

Gamemaster Rewards

Gamemaster nodes earn a share of transaction fees from PTX rounds they participate in. Rewards are distributed through a daily lottery across all nodes that participated honestly in the preceding 24-hour window. Each honest round participation earns one lottery ticket.

This lottery design eliminates the per-round attack incentive: no Gamemaster can predict whether any specific round will generate a reward for them. The financial incentive to manipulate an individual round is eliminated by design. Non-participation results in PoSe score accumulation and forfeiture of lottery tickets for the window.

Launch and Exchange

Hemis launched with a public airdrop, distributing coins broadly to ensure no single party controls the network. The launch was designed to avoid both the vulnerabilities of a stealth launch (51% and Sybil attack exposure) and the costs and legal risks of a coin sale.

The launch followed four stages: a private but fully transparent chain setup; public GitHub access for community download; a coin airdrop to stakers; and handoff once more than half of staking wallets were outside core team control.

HMS is listed on NonKYC. As the project matures and community engagement grows, listings on larger and higher-profile exchanges are a natural progression. The strongest signal to exchanges is an active, engaged community.

Get Involved

Game developers: API documentation and SDK will be available at Phase 4 launch. The goal is that any developer who can make an HTTP call can integrate Hemis into their game.

Node operators: Run a Gamemaster node and earn rewards from games built on the network. 410 nodes are currently active. The more independent operators on the network, the stronger the fairness guarantees for every game.

Players: Any game built on Hemis gives you the ability to independently verify every result. The proof is permanent, public, and requires no specialist knowledge to check.

Community: Follow development updates on the Hemis Website and Hemis Discord. Phase 0 is complete. Phase 1 is beginning.

Hemis

Simple tools for popular games.