

GemStep (GemS)

A Verifiable Move-to-Mint Protocol
for On-Chain Wellness Rewards

What's inside

- Step submission lifecycle and verification flow
- Fraud prevention and monitoring
- Tokenomics and emission discipline
- Cross-chain governance and emergency controls

Whitepaper v1.0
September 2026

www.gem-step.com

NON-CUSTODIAL • VERIFIABLE • GOVERNANCE-CONTROLLED

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute financial, investment, legal, or tax advice. Nothing contained herein shall be construed as an offer, solicitation, or invitation to buy, sell, or otherwise acquire any digital asset, security, or financial instrument in any jurisdiction.

The GemStep protocol and any associated digital assets are designed for utility within a blockchain-based wellness rewards system. No representations or guarantees are made regarding future performance, value, or adoption.

Readers should conduct their own independent research and consult with qualified professional advisors before making any financial, investment, or operational decisions. Participation in blockchain networks and digital asset systems involves risk.

Additional disclosures and risk considerations are set out in the **Disclaimers & Disclosures** section of this document.

GemStep (GemS) Whitepaper

A Verifiable Move-to-Mint Protocol for On-Chain Wellness Incentives

Version 1.0

Contents

1.	Executive Summary	4
2.	Market Opportunity	5
2.1	The Problem	5
2.2	Why Verifiable Wellness Matters.....	5
2.3	Comparison to Centralized Alternatives	5
3.	Step Submission Lifecycle	5
3.1	Actors	5
3.2	Submission Flow.....	6
4.	System Architecture	6
4.1	Device Trust Layer	6
4.2	Verification API (Optional)	7
4.3	On-Chain Execution Guarantees.....	7
5.	Validation Layer	7
6.	Cryptographic Verification Framework	8
6.1	EIP-712 Typed Data	8
6.2	Merkle Proof Aggregation.....	8
6.3	Device Attestation	8
6.4	Signature Paths	8
7.	Fraud Prevention & Monitoring.....	9
8.	Reward Logic and Tokenomics	9
8.1	Emission Model.....	9
8.2	Supply Discipline	9
8.3	Economic Attack Resistance.....	9
9.	Governance & Cross-Chain Security	10
9.1	Two-Tier Authority Structure.....	10
9.2	Cross-Chain Architecture	10

9.3	Timelock Guarantees	10
10.	Threat Model & Security Assumptions	10
10.1	Adversarial Scenarios	10
10.2	Explicit Assumptions	11
11.	Integration & Roadmap	11
11.1	Client Integration Patterns	11
11.2	Use Cases	11
11.3	Future Upgrades	11
12.	Conclusion	11
Appendix		12
	Glossary	12
	Abbreviations	12
13.	Disclaimers & Disclosures	13

1. Executive Summary

GemStep is a decentralized protocol that transforms authenticated human movement into verifiable on-chain rewards. By combining cryptographic verification, layered fraud prevention, and transparent tokenomics, GemStep bridges off-chain wellness activity with blockchain-native incentive mechanisms. The protocol is designed for scalability, security, and broad applicability across corporate wellness programs, insurance incentives, and Web3 fitness ecosystems.

At its core, GemStep implements a hybrid Layer-1 / Layer-2 security architecture that deliberately separates emergency response authority from routine governance. This separation enables rapid intervention during critical events while preserving deliberate, transparent protocol evolution over time.

Emergency controls leverage Ethereum Layer-1 finality to enable near-instant threat mitigation, while governance actions are subject to mandatory delay periods and transparent execution via cross-chain timelock mechanisms. Combined with EIP-712 signed submissions, device-source verification, and anomaly detection, GemStep establishes a new standard for verifiable, incentive-aligned wellness on-chain.

2. Market Opportunity

2.1 The Problem

Most existing wellness platforms operate as centralized systems that lack transparency, portability, and verifiability. User activity data is siloed, reward calculations are opaque, and participants must trust proprietary systems without independent auditability. These limitations erode user confidence and restrict the design of incentive programs.

At the same time, the global corporate wellness market is projected to exceed \$100 billion by 2030, driven by growing demand for measurable health outcomes and performance-linked incentives (McKinsey; Global Wellness Institute). The absence of a verifiable, interoperable infrastructure remains a critical bottleneck to scalable adoption.

2.2 Why Verifiable Wellness Matters

Verifiable wellness infrastructure unlocks new economic and behavioral alignment across stakeholders:

- **Economic Alignment:** Tamper-resistant activity data enables insurers, employers, and protocols to design incentive structures with materially reduced fraud risk.
- **User Sovereignty:** Individuals retain control over their activity data and may permission its use across multiple applications without vendor lock-in.
- **Interoperability:** A standardized verification layer enables cross-platform reward portability and composability.

2.3 Comparison to Centralized Alternatives

Aspect	Centralized Platforms	GemStep Protocol
Data Ownership	Platform-controlled	User-controlled
Reward Transparency	Opaque	On-chain, auditable
Interoperability	Limited	Cross-application via open standards
Fraud Resistance	Proprietary, non-verifiable	Cryptographic, publicly verifiable

3. Step Submission Lifecycle

GemStep defines a deterministic, multi-stage lifecycle for converting off-chain human movement into on-chain rewards. Each submission is authenticated, replay-safe, and processed under uniform protocol rules before any GemS tokens are minted.

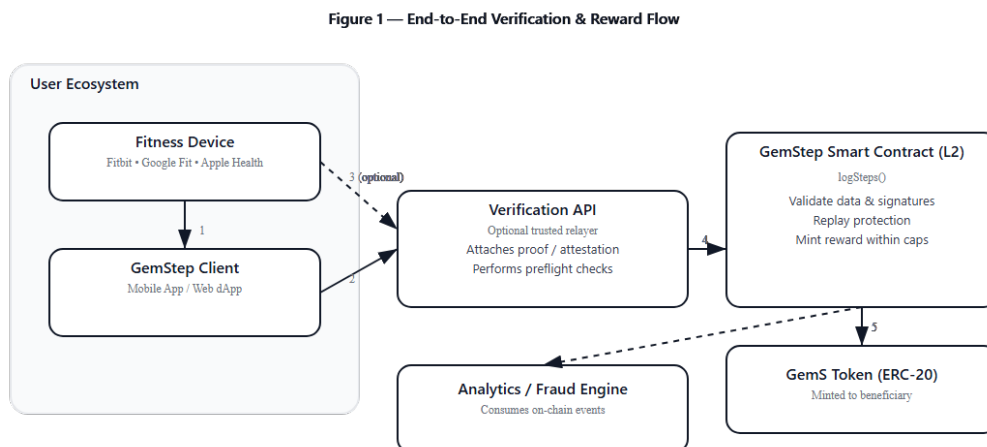
3.1 Actors

- **User:** The wallet address (EOA or ERC-1271 contract wallet) associated with the individual generating activity data.
- **Beneficiary:** The address designated to receive minted GemS tokens. This may differ from the user to support delegated rewards, custodial vaults, or pooled programs.
- **Verification API (Optional):** A whitelisted relayer authorized to submit verified payloads on behalf of users.
- **Device:** A fitness device or API source (e.g., Fitbit, Google Fit, Apple Health) providing authenticated motion data.

3.2 Submission Flow

1. **Step Collection:** Movement data is accumulated off-chain from an approved source.
2. **Payload Construction:** The client constructs a StepSubmission payload containing the user, beneficiary, step count, nonce, deadline, source identifier, and version.
3. **Signature Generation:** An EIP-712 typed-data digest is generated and signed by the user or an authorized signer.
4. **Verification Bundle:** Optional Merkle proofs or device attestations are attached.
5. **On-Chain Execution:** The payload is submitted to the logSteps() function, which validates inputs, verifies authenticity, and mints rewards atomically.

The end-to-end lifecycle is illustrated in **Figure 1 — End-to-End Verification & Reward Flow**.



4. System Architecture

4.1 Device Trust Layer

The Device Trust Layer defines which data sources are eligible for participation:

- **Approved Sources:** Whitelisted devices and APIs with authenticated data export capabilities.
- **Attestation Requirements:** Hardware-bound attestations for higher-value or medical-grade sources.
- **Source Versioning:** Each source is versioned to accommodate firmware updates and evolving data formats.

4.2 Verification API (Optional)

The Verification API serves as an optional, trusted relay:

- **Role:** Aggregates and batches submissions to reduce gas costs for users.
- **Trust Assumptions:** Relayers are whitelisted and must comply with protocol rules and privacy constraints.
- **Merkle Batching:** Periodic Merkle root updates enable efficient proof-based verification of batched submissions.

4.3 On-Chain Execution Guarantees

- **Atomic Validation:** Validation, verification, and minting occur within a single transaction.
- **Event Emission:** Comprehensive events enable real-time monitoring and analytics.
- **Deterministic Outcomes:** Given identical inputs, the protocol always produces the same state changes.

5. Validation Layer

Before cryptographic verification occurs, GemStep enforces strict validation rules to ensure payload correctness and protocol compatibility.

Validation includes:

- Non-zero beneficiary address
- Step count within configured limits (e.g., 0–10,000 steps per day)
- Valid deadline within the signature validity window
- Approved data-source identifier
- Supported payload version

This layer prevents malformed or outdated submissions from consuming verification resources.

6. Cryptographic Verification Framework

GemStep employs a layered cryptographic model to authenticate activity and prevent forgery or replay. The interaction between signatures, proofs, and attestations is illustrated in **Figure 1**.

6.1 EIP-712 Typed Data

All submissions are signed using EIP-712 typed data, binding the payload to the chain ID, verifying contract, and protocol version. This prevents cross-chain and cross-contract replay attacks.

Example Domain:

```
{  
  "name": "GemStep",  
  "version": "1.0",  
  "chainId": 42161,  
  "verifyingContract": "0x..."  
}
```

6.2 Merkle Proof Aggregation

For batched or oracle-based integrations, Merkle roots may be configured per data source. Each submission includes a proof verifying inclusion under the active root.

Rationale: Merkle aggregation reduces on-chain storage and gas costs while preserving cryptographic integrity.

6.3 Device Attestation

Certain sources require hardware-bound attestations confirming that reported activity originated from a trusted device. Attestations are versioned and protected against replay.

6.4 Signature Paths

GemStep supports:

- EOA signatures
- Verification API signatures (whitelisted relayers)
- ERC-1271 contract wallet validation

Replay-Prevention Matrix

Attack Vector	Mitigation
Cross-chain replay	EIP-712 chain-ID binding
Cross-contract replay	Verifying contract in digest
Duplicate submission	Nonce tracking + deadline enforcement

7. Fraud Prevention & Monitoring

Following successful verification, GemStep invokes abstract fraud-prevention hooks:

- **Rate Limiting:** Per-user, per-source, or global limits.
- **Anomaly Detection:** Statistical detection of improbable activity patterns.
- **AI-Driven Analysis (Future):** Machine-learning-based behavioral analysis.

These mechanisms are upgradeable without modifying core verification logic.

8. Reward Logic and Tokenomics

8.1 Emission Model

Verified steps are converted into GemS rewards using deterministic formulas:

$$\text{Reward} = \text{BaseRate} \times \text{StepCount} \times \text{Multiplier}$$

Multipliers may adjust for source trust tier, user reputation, or promotional programs.

8.2 Supply Discipline

- **Monthly Caps:** Maximum rewards per user per month.
- **Halving Schedule:** Periodic emission reductions (e.g., every 24 months).
- **Absolute Supply Cap:** Fixed maximum GemS supply.

8.3 Economic Attack Resistance

- **Sybil Resistance:** Requires authenticated device sources.
- **Inflation Bounds:** Emission caps prevent unbounded issuance.
- **Long-Term Viability:** Halving ensures sustainable reward distribution.

9. Governance & Cross-Chain Security

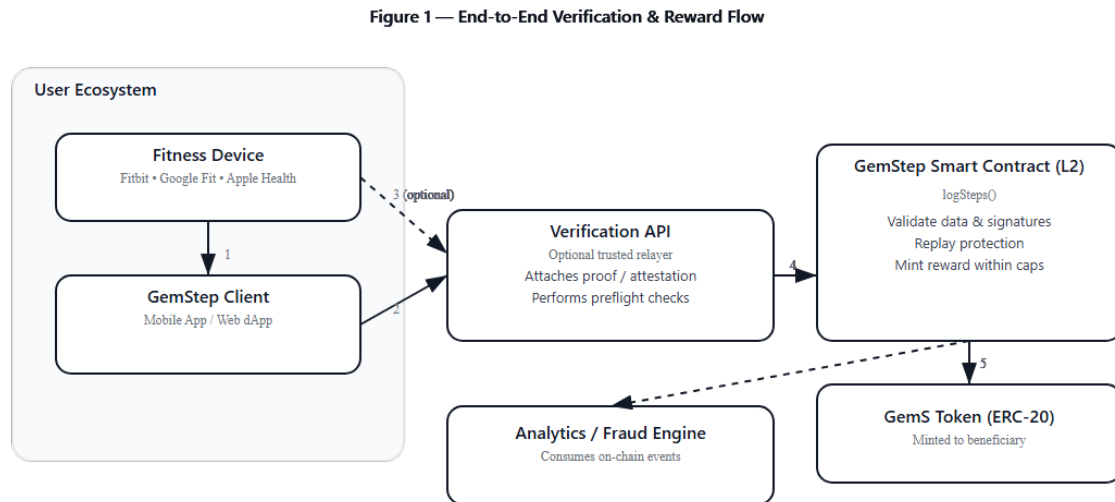
9.1 Two-Tier Authority Structure

- **Emergency Controls:** Rapid response actions such as pausing minting.
- **Governance Actions:** Protocol upgrades, parameter changes, and source management.

9.2 Cross-Chain Architecture

- **Ethereum L1:** Anchors governance and emergency authority.
- **Arbitrum L2:** Executes verification and minting for low-cost, high-throughput activity.

(Illustrated in Figure 2 — Cross-Chain Governance & Emergency Control Flow)



9.3 Timelock Guarantees

All governance actions are subject to timelock delays, allowing users to react before changes take effect. Governance cannot retroactively modify or invalidate already verified submissions or minted rewards.

10. Threat Model & Security Assumptions

10.1 Adversarial Scenarios

Scenario	Mitigation
Forged device data	Hardware attestations + source whitelisting
Replay attacks	EIP-712 + nonce and deadline enforcement

Governance abuse	Timelocks + multisig thresholds
Oracle manipulation	Anomaly detection + fallback sources

10.2 Explicit Assumptions

- Cryptographic primitives remain secure.
- Approved devices are not universally compromised.
- Governance participants act in good faith.

11.Integration & Roadmap

11.1 Client Integration Patterns

- **Direct Integration:** Wallets sign and submit payloads directly.
- **API Relay:** Gas-optimized submission via Verification API.
- **Enterprise SDK:** Simplified integration for corporate programs.

11.2 Use Cases

- Corporate wellness incentives
- Insurance health rewards
- Web3 fitness ecosystems

11.3 Future Upgrades

- Zero-knowledge verification
- Multi-chain expansion
- Dynamic reward curves

12.Conclusion

GemStep provides a secure, scalable foundation for verifiable wellness incentives by aligning authenticated human activity with on-chain economic value. Through cryptographic verification, disciplined tokenomics, and transparent cross-chain governance, the protocol enables trustless, interoperable wellness rewards suitable for enterprise and Web3 adoption.

Appendix

Glossary

- EOA: Externally Owned Account (standard Ethereum wallet)
- ERC-1271: Standard for contract wallet signature validation
- Merkle Proof: Cryptographic proof of set membership
- Attestation: Hardware-signed statement of data authenticity

Abbreviations

- GemS: GemStep Token
- L1: Layer 1 (Ethereum Mainnet)
- L2: Layer 2 (Arbitrum)
- EIP: Ethereum Improvement Proposal

13. Disclaimers & Disclosures

1. No Investment Advice or Offering

This document is not intended to constitute, and shall not be construed as, financial, investment, legal, regulatory, or tax advice. Nothing in this whitepaper constitutes an offer, solicitation, or recommendation to purchase, sell, or hold any digital asset or financial instrument.

No part of this document shall form the basis of, or be relied upon in connection with, any investment decision or contractual relationship.

2. Utility-Focused Design

Any digital assets associated with the GemStep protocol are intended solely for functional use within the protocol, including participation in verifiable wellness reward mechanisms and related on-chain processes.

No rights to equity, dividends, revenue share, or ownership interests in any entity are conveyed by holding or using such assets.

3. No Guarantees

The GemStep protocol, associated software, and smart contracts are provided on an “as-is” and “as-available” basis. No representations, warranties, or guarantees are made regarding functionality, security, availability, performance, or future development.

There is no assurance that the protocol will meet user expectations, remain operational, or achieve any particular level of adoption.

4. Regulatory Uncertainty

Blockchain technologies and digital assets may be subject to evolving regulatory frameworks across jurisdictions. Regulatory actions or interpretations may materially impact the development, deployment, or use of the GemStep protocol or associated digital assets.

Participants are responsible for understanding and complying with applicable laws and regulations in their respective jurisdictions.

5. Technical and Operational Risks

Use of the GemStep protocol involves inherent risks, including but not limited to:

- smart contract vulnerabilities
- network congestion or failures
- protocol upgrades or parameter changes
- third-party dependencies
- cybersecurity threats

While reasonable measures are taken to mitigate such risks, no system can be guaranteed to be free from defects or exploits.

6. Forward-Looking Statements

This whitepaper may contain forward-looking statements, including statements regarding future functionality, governance, or adoption. Such statements are based on current expectations and assumptions and are subject to risks and uncertainties that could cause actual outcomes to differ materially.

No obligation is undertaken to update or revise any forward-looking statements.

7. Limitation of Liability

To the maximum extent permitted by law, the authors, contributors, and maintainers of the GemStep protocol shall not be liable for any direct or indirect losses, damages, or claims arising from the use of, or reliance upon, this whitepaper or the protocol described herein.