Streak Token — Whitepaper v1.0.1 (First Public Release)

A Sybil-Resistant Streak-to-Earn Protocol on World Chain

Version: 1.0.1
Date: 2026-01-01

Launch Details

- Protocol Launch Date: 2025-10-08, 14:52:05 (UTC −07:00)
- Network: World Chain
- Contract Address: 0xa786B581D750cC81953239BC130d169a16F87779
- Block: 20312343

Release Notes (First Public Release)

*This document is the **first public whitepaper** for Streak Token. It consolidates the protocol's original design and incorporates the current roadmap, including:*

- *the **burn program** for the initial owner mint, and*
- *the **~3-year governance handoff** to DAO governance.*

Abstract. *Streak Token introduces an on-chain streak-to-earn protocol deployed on World Chain, a human-first Ethereum Layer 2 network built with the OP Stack. World Chain is engineered to prioritize blockspace and gas access for World ID–verified users, making it an ideal environment for applications based on proof of personhood. Streak Token utilizes World ID, a privacy-preserving proof-of-personhood protocol, enabling users to demonstrate uniqueness as humans via zero-knowledge proofs, without disclosing their identity. World ID verification is achieved through the Orb, a biometric device that scans a user's face and irises to confirm uniqueness. Biometric images are processed and stored encrypted on the user's device, with only derived codes retained to prevent duplicate registrations.*

The protocol encodes streak progression, timing rules, milestone rewards, cycle bonuses, and sybil resistance directly within its smart contract. The structure is as follows:

- *One verified human is assigned one streak and one reward stream*
- *Claims are permitted once every 24–36 hours*
- *Streaks progress in 30-day cycles with fixed milestones*
- *Rewards are minted on-chain as an ERC-20 token (STREAK)*

By linking token issuance to verified human streak behaviour, Streak Token establishes a novel, identity-aware token distribution method.

Fairness Commitments & Progressive Decentralization. *Streak Token is designed to be maximally fair over time through (i) sybil-resistant distribution to verified humans and (ii) a progressive decentralization plan. While the contract initialized with a 1,000,000 token owner mint for bootstrap purposes, the roadmap commits to burning this allocation such that circulating supply becomes community-minted. In addition, administrative control is time-bounded: after a ~3-year transition, ownership is automatically renounced or transferred to DAO governance, enabling the community to steer future parameters and upgrades through transparent processes.*

Table of Contents

1. Introduction

Daily streak mechanics are a common feature in consumer applications such as language learning, fitness, and gaming. However, these systems often exhibit several shortcomings:

- Centralization: Streak data is retained in proprietary databases
- Opacity: Reward logic is not open for public scrutiny
- Sybil vulnerability: It is easy to create multiple accounts
- Lack of composability: Off-chain streaks cannot be utilized across different applications

Streak Token offers a new approach by incentivizing verified human consistency with an on-chain ERC-20 token, ensuring that both identity and streak logic are enforced by smart contracts. Key features include:

- On-chain tracking of streaks, removing reliance on private databases
- Deterministic contract code mints rewards
- Identity secured by World ID proofs
- User interaction via World App on World Chain

This protocol serves as a foundation for human-centric reward systems, habit-formation tools, and sybil-resistant distribution models.

2. Background: World Chain, World App, and World ID

2.1 World Chain: A Human-First Layer 2

World Chain is a Layer 2 blockchain constructed on the OP Stack and is a part of the Optimism Superchain. It maintains compatibility with the Ethereum Virtual Machine (EVM) and derives security from Ethereum, while optimizing for applications that depend on proof of personhood and identity. World Chain is described as "human-first," with features such as:

- Prioritizing blockspace for World ID–verified individuals
- Providing gas optimizations or allowances for verified users
- Aiming to reduce bot activity and automated abuse

This environment is particularly suitable for Streak Token, as fairness relies on restricting rewards to unique humans and maintaining affordable daily interactions.

2.2 World App: Wallet and Miniapp Platform

World App, created by Tools for Humanity, serves as the main wallet and interface for the World ecosystem. It enables users to:

- Securely store and manage their World ID locally on their mobile device
- Send and receive digital assets such as USDC and other tokens
- Access a variety of Mini Apps, including DeFi, payments, games, and utilities

Mini Apps are deployed on World Chain, positioning World App as the frontend for a growing decentralized application ecosystem. Streak Token is designed to function as a Mini App within World App, offering users:

- A wallet for transactions
- Secure storage for World ID
- The main interface for daily claims and streak visualization

2.3 World ID and the Orb

World ID is a privacy-preserving proof-of-personhood protocol, allowing users to prove their humanity and uniqueness online using zero-knowledge proofs, without disclosing personal identifiers such as names or raw biometrics. Essential concepts include:

- Zero-Knowledge Proofs (ZKPs): Users create proofs confirming their inclusion in a valid identity set without revealing their specific identity
- Nullifier Hash: A unique value derived from the user, app ID, and action, ensuring each proof is used only once for a specific action, without linking to the underlying identity

World ID supports several verification methods:

- Orb verification: High-assurance biometric verification through a dedicated device called the Orb

- Alternative methods (such as phone verification) for broader accessibility at lower assurance

The Orb is a biometric device that captures images of the user's irises and face, processes them to produce cryptographic codes for uniqueness verification, and stores the biometric images encrypted on the user's device. Only the derived codes are retained to prevent duplicate registrations. Upon successful Orb verification, the user's World ID is stored in the World App, enabling them to sign in to compatible applications and generate zero-knowledge proofs of personhood as required.

2.4 How the World Stack Empowers Streak Token

Streak Token takes advantage of three elements within the World stack:

- Verified uniqueness: High-assurance identity via World ID and the Orb ensures each identity is linked to a single human
- On-chain enforcement: EVM compatibility of World Chain allows streak logic to be fully encoded in smart contracts
- Accessible user experience: World App provides a mainstream wallet and app platform, simplifying daily user interactions

The Streak Token contract uses World ID nullifier hashes to track streaks, not raw wallet addresses. Verification occurs on-chain through the IWorldID interface, aligning the protocol logic with the guarantees provided by the underlying identity system.

3. Claim of Novelty

Streak Token represents, to the best of our knowledge, the first protocol to combine the following aspects:

- Streak mechanics as the core protocol function, focusing primarily on daily streak tracking and rewards
- Comprehensive on-chain enforcement of streak timing, length, cycle completion, and bonus rules through smart contracts on World Chain
- Mandatory World ID Orb verification for claiming rewards, restricting successful minting to verified humans
- Identity-bound streak state keyed by nullifier hash, ensuring each World ID manages exactly one streak, independent of wallet changes
- Transparent ERC-20 token issuance linked to streak events, with all emissions observable and auditable on-chain

Previous applications may have used streak mechanics or incentivized engagement, but they typically operate off-chain, lack robust sybil resistance, and do not combine biometric proof of personhood with on-chain streak and token minting. Streak Token is the first to realize this combination as a public smart contract on World Chain.

4. System Architecture

4.1 Components

- StreakToken Contract (ERC-20, upgradeable):
- Tracks streaks and cycles per World ID nullifier hash
- Enforces timing windows (24h wait plus 12h grace)
- Mints base, milestone, and bonus rewards
- Integrates with IWorldID for proof verification

World ID Verification Service:
Verifies zero-knowledge proofs
Ensures nullifiers are not reused for the same external nullifier
World App Miniapp:
Enables users to generate World ID proofs
Submits claims to the StreakToken contract
Displays streak status, next claim time, and projected rewards

4.2 Data Model

For each nullifier hash (representing a unique identity), the contract maintains the following structure:

```
struct MintData {
uint40 lastMintedAt;
uint32 numOfMints;
uint32 streak;
uint32 completedCycles;
}
```

The state is updated with every successful mint operation.

5. Streak Mechanics

5.1 Claim Timing

Claim timing is governed by two parameters:

- waitBetweenMints: Default is 24 hours
- gracePeriod: Default is a total of 36 hours from the last claim

The rules are as follows:

- If the time since the last mint is less than waitBetweenMints, the transaction is reverted with an error
- If the time since the last mint exceeds gracePeriod and the streak is greater than zero, the streak is considered broken:
- The streak resets to one
- A StreakBroken event is emitted

Therefore, the safe window to claim is between 24 and 36 hours after the previous claim.

5.2 30-Day Streak Cycles & Milestones

The protocol defines fixed milestone days within a 30-day streak cycle:

- Day 3
- Day 7
- Day 12
- Day 20
- Day 30

On each successful claim, the streak counter increases (or resets to one after a break). When the streak reaches 30:

- The completedCycles counter increases
- A CycleCompleted event is emitted
- A cycle bonus may be awarded
- The streak counter resets to zero, starting a new 30-day cycle

6. Token Issuance Model

6.1 Base Reward

For each successful claim that is not on a milestone day, the user receives one STREAK token.

6.2 Milestone Rewards

On milestone days (3, 7, 12, 20, and 30), the reward is multiplied by the day number:

Streak Day	**Reward**
3	3 STREAK
7	7 STREAK
12	12 STREAK
20	20 STREAK
30	30 STREAK

6.3 Cycle Bonuses

Upon completing a 30th streak (i.e., day 30), the completedCycles counter increments by one. Every third completed cycle (when completedCycles is divisible by three), an additional 100 STREAK tokens are minted as a cycle bonus. The streak counter then resets to zero.

6.4 Design Considerations

- A fixed set of milestones and a uniform base reward simplify the model
- Large, predictable boosts at milestones and every third cycle encourage continued engagement
- All emission rules are contained in the open-source contract for transparency and auditability

7. Tokenomics

7.1 Initial Supply

At contract initialization, 1,000,000 tokens (scaled by the number of decimals) are minted to the owner's address. No user balances are pre-allocated; users earn tokens solely through mint operations.

7.2 User Emissions

User emissions are composed of daily base rewards, milestone rewards, and a 100 STREAK cycle bonus every three completed 30-day cycles. Emissions are naturally limited by:

- One claim permitted per 24–36 hours
- The number of verified identities
- The challenge of maintaining long streaks

7.3 Owner Minting and Cap

The contract allows the owner to mint tokens, but only before a set transition timestamp and with strict limitations. The total owner supply, including the initial allocation, cannot exceed 5% of the total tokens minted to users. Any attempt to exceed this cap results in a transaction revert.

7.4 Governance Transition

A transition timestamp is set during initialization. Prior to this timestamp, upgrade authorization and administrative actions are restricted to the owner role. After the timestamp, authority shifts to **DAO governance** (the designated community governor). Owner minting is disabled post-transition (as implemented), and long-term control is aligned with governance rather than a permanent admin key. Governance actions are expected to be transparent and auditable, with timelocks and proposal/vote processes where applicable.

7.5 Fair Launch Commitments & Burn Program

Ownership Fairness. Streak Token aims to be fully community-owned long-term. There are **no investor allocations**, and the intended steady-state is **0% team allocation**. All participation should occur through the same public mint rules enforced on-chain.

Initial Owner Mint. At initialization, 1,000,000 tokens were minted to the owner address to bootstrap deployment, liquidity, operational execution, and early ecosystem development.

Burn Roadmap (Next ~90 Days). To align with the goal of long-term community ownership, the protocol commits to removing the initial owner mint from circulation via a two-step burn plan:

- **Step 1 — Immediate Burn:** burn **700,000** tokens from the initial owner allocation.
- **Step 2 — Completion Burn:** burn the remaining **300,000** tokens once the community has minted an additional **1,000,000** tokens through normal participation.

Outcome. After completion, the initial 1,000,000 owner mint will be permanently removed, and circulating supply will be dominated by tokens minted through verified human participation.

Transparency. Burn transaction hashes and updated supply snapshots will be published and maintained in a public ledger (Appendix B).

7.6 Progressive Decentralization & 3-Year Governance Handoff (DAO)

Streak Token follows a progressive decentralization model. Early-stage administration exists to ensure safety and operational stability while the system matures; however, this control is intentionally time-bounded.

Admin Sunset (~3 Years). A transition timestamp is set at initialization. At approximately the three-year mark, administrative ownership is **automatically renounced or transferred** (as implemented in the contract), removing perpetual founder control.

DAO Governance. After the transition, control shifts to **DAO governance**, a community-led mechanism intended to represent token-holder interests. Governance may steer protocol evolution through transparent actions such as parameter updates (where supported) and community-approved upgrade/migration processes (if deeper changes are required).

Safety Rails. Governance actions should be subject to:

- public proposals and defined voting windows,
- execution timelocks where applicable,
- on-chain traceability and auditable records.

This model is intended to ensure that long-term control belongs to the community, not any individual operator.

8. Sybil Resistance

Streak Token employs two layers of sybil resistance:

- World ID layer (off-chain and protocol level):
- Each World ID corresponds to a unique individual
- Orb verification provides high assurance

Smart contract layer (on-chain enforcement):
WORLD_ID.verifyProof(...) is invoked during mint operations with relevant parameters
Ensures the proof is valid for the provided signal
Nullifier hashes are checked for prior use
Links the signal to the sender's wallet address
This dual-layered approach ensures one identity controls one streak and one reward stream, prevents proof replay, and mitigates multi-account farming at the identity level rather than merely the wallet level.

9. Technical Specification

9.1 Core Contract Interfaces

- mint(address signal, uint256 root, uint256 nullifierHash, uint256[8] calldata proof):
- Verifies claim timing
- Calls WORLD_ID.verifyProof(...)
- Ensures the signal matches the sender's address
- Updates MintData and mints rewards

claimStatus(uint256 nullifierHash): Returns information on last mint time, current streak, completed cycles, remaining wait time, streak risk status, and next milestone
getMintData(uint256 nullifierHash): Retrieves the full MintData structure
canClaimNow(uint256 nullifierHash): Checks if the waiting period has elapsed
secondsUntilNextClaim(uint256 nullifierHash): Returns remaining seconds before the next claim is permitted
Other view helpers are provided for front-end integration
Upgrade and governance management functions are implemented (details omitted for brevity)

9.2 Upgradeability & Safety

The contract employs OpenZeppelin's UUPSUpgradeable pattern for upgradeability, OwnableUpgradeable for ownership management, and ReentrancyGuardUpgradeable to secure mint and ownerMint functions. Upgrades are permitted only by authorized parties, with governance transitioning as described previously.

10. Roadmap

Phase 0 — Protocol Launch:

- Deploy StreakToken on World Chain
- Release the World App Mini App with core claim, streak display, and history features.

Phase 1 — Fairness Reset (Next ~90 Days):

- Execute the burn program for the initial owner mint (Step 1 burn + Step 2 completion burn).
- Publish burn transaction hashes and a public supply/burn ledger.
- Publish a governance handoff schedule and high-level governance process.

Phase 2 — Ecosystem Integration:

- Develop public APIs and SDKs to integrate Streak Token with other Mini Apps.
- Explore further governance mechanisms for emission and utility adjustments.

Phase 3 — Governance Handoff (~3-Year Mark):

- Trigger the admin sunset (ownership renounced/transferred as implemented).
- DAO governance becomes the sole authority for upgrades/parameters.
- Introduce governance safety rails (timelock + proposal/vote transparency) as required.

11. Use Cases

- Sybil-Resistant Loyalty & Rewards: Reward customers based on verified human participation and sustained engagement
- Habit-Building Applications: Enable health, education, or productivity apps to leverage Streak Token's on-chain streak primitives
- Fair Airdrops and Distribution Schemes: Employ streak-based participation as a criterion for additional token distributions or governance rights

12. Conclusion

Streak Token leverages the World stack—comprising World Chain, World App, World ID, and the Orb—to establish a novel on-chain primitive: verified human consistency as an economic asset. By encoding streak mechanics, milestone rewards, and cycle bonuses in a contract keyed by World ID nullifiers, the protocol ensures that rewards are allocated to real humans, emissions are transparent and verifiable, and identity is preserved in a privacy-conscious manner. This foundation supports a new generation of identity-aware applications in finance, gaming, and social coordination on World Chain.

13. Appendix A — Deployment Details

- Network: World Chain
- Contract Address: 0xa786B581D750cC81953239BC130d169a16F87779
- Block: 20312343
- Token Symbol: STREAK
- Token Name: Streak Token
- Decimals: As configured in ERC20Upgradeable at initialization (typically 18)
- World ID Group ID: 1
- External Nullifier: Calculated as hashToField(hashToField(appId) ‖ actionId), derived on-chain as specified in the contract