TIME Humanity Protocol Whitepaper

English edition: 6 November 2026. Policy content: 2 November 2026. Historical evidence retains its original dates; no new issuance or audit is implied.

Research v0.1 · 2026-11-02

01 / PROJECT THESIS: Private eligibility for trusted participation.

TIME Humanity Protocol researches how applications can verify participation eligibility while reducing access to persistent identity information. Intended contexts include community governance, surveys and open collaboration. These are proposed integrations, not existing customers, revenue or verified users.

Protocol capabilities and transferable assets are designed separately. Anonymous membership proofs answer whether a member meets activity rules; TIME belongs to the asset layer. Holding tokens does not establish human eligibility, and token amounts do not count human identities.

02 / LAYERED ARCHITECTURE: Give every capability an explicit trust boundary.

The uniqueness layer explores synthetic-data deduplication. Eligibility management researches issuance, suspension, revocation and recovery. The proof layer uses Semaphore; applications define participation scopes and reject duplicates. The asset layer separately handles transfers, vesting and supply policy.

No complete real-human uniqueness system exists. Biometric capture, liveness, real deduplication, anonymous issuance and private recovery after secret loss remain unresolved. Research uses synthetic identities only; prototype results do not justify collecting real biometric identities.

03 / ELIGIBILITY & REPLAY PROTECTION: Prove membership within a defined participation scope.

The implementation actually generates and verifies Semaphore/Groth16 proofs, without substituting a mock verifier. Application, activity and epoch define an explicit scope. Membership roots establish eligibility but are not replay domains, so membership changes do not reset activity nullifiers.

The Node/SQLite reference uses transactions and unique keys for concurrent scope/nullifier submissions. The browser demo retains session records only; refresh can reset them. It is not persistent, network-wide replay protection.

Different application nullifiers support a specific scope-separation conclusion. IP, timing, messages, small groups and issuance/recovery logs can still correlate participants. These tests must not be described as comprehensive system unlinkability.

04 / TIME ASSET POLICY: 1.4 billion initial tokens. One TIME per net person of decline.

The project has confirmed 1,400,000,000 initial TIME tokens with 18 decimals. This is an issuance design, not current mainnet supply; no official mainnet token exists. Allocations, vesting, treasury, liquidity budget and specific utility remain undecided.

The confirmed rule uses China's annual net population decline: each net person of decline corresponds to one TIME burned through manual administrator execution. Flat or rising population causes no burn and no mint. First data year and reserve allocation remain undecided.

The historical draft accepts supply as a constructor argument and has no built-in 1.4 billion constraint, population burn entry point or off-chain submission mechanism. Historical bytecode and vesting packages do not implement the new policy. A separate TIMEAnnualBurnToken candidate fixes initial supply at 1.4 billion, burns a dedicated reserve, prevents duplicate annual finalization and uses two-step administrator transfer. It passed local EVM tests but has no official deployment.

05 / POPULATION-LINKED BURNS: Data, formula and execution are separate questions.

China's National Bureau of Statistics reported 1,408,280,000 people at end-2024 and 1,404,890,000 at end-2025, a decline of 3,390,000. The scope covers mainland China's 31 provincial-level regions and active-duty military personnel, excluding resident Hong Kong, Macao and Taiwan residents and foreign nationals. These sources do not endorse TIME.

A historical calculation under the confirmed rule maps the 2025 decline of 3,390,000 people to 3,390,000 TIME. This is neither approved retroactive burning nor an executed transaction. Statistics published in ten-thousand-person units must first be multiplied by 10,000. The contract accepts whole people and converts tokens to 18-decimal base units.

Burning should use only a dedicated, actually funded reserve; ordinary wallets and pools are not directly debited. A reserve shortfall must be disclosed, never reported as a completed burn or filled through invented issuance. The reserve allocation is undecided. The candidate accepts reserve funding by token transfer and has no reserve withdrawal entry point. Do not deploy it on production networks without review.

The administrator executes annual finalization manually; no automatic population oracle is provided. Inputs are the data year, whole-person year-end population and evidence hash. The contract calculates decline from the previous year's population; the administrator cannot specify an arbitrary burn amount. A hash neither authenticates data nor guarantees file availability, and the contract cannot read statistics webpages. Source versions, year/units, revisions, independent checking, disclosure delays and duplicate protection require operational controls. Flat or rising population records zero burn and advances the year; later declines use the previous actual figure, so a decline after a rebound also burns. Missing reports do not advance the year. Methodology changes and corrections to finalized records require further governance. Data year and publication date differ; no automatic 1 January burn is promised.

Supply decreases require burn logic that reduces totalSupply and emits inspectable events. Sending tokens to a so-called dead address does not itself reduce reported contract supply. Burning guarantees no demand, price, volume or return.

06 / GOVERNANCE & CONTROL: Turn commitments into inspectable constraints.

Treasury, multisig, vesting, reserve and data-submission roles need separate decisions. Multisig reduces single-key risk but does not imply vesting, independent governance or correct statistics. No verified official signers, operating entity or governance scheme are available for disclosure.

The vesting reference supports cliff-based catch-up followed by linear vesting. Beneficiary rights are transferable, later funding follows the original timeline, and revocation/upgrade recovery is absent. An empty contract locks no assets. No official team assets have been funded into vesting.

07 / ENGINEERING EVIDENCE: Tests need an explicit execution context.

The website/real-ZK reference retains 18 recorded tests. A separate historical deployment package passed six groups on Windows and actual Linux/Docker. Vesting checks covered five schedules and 182 timestamps. Counts belong to their own versions and scopes, not a combined production-security rating.

Container checks exercised non-root execution, read-only root filesystem, loopback networking and no extra effective capabilities. Deployment verification uses actual local-EVM positive records; bad-receipt cases explicitly inject faults. Public-testnet checks read chain and blocks only; no real-wallet deployment acceptance exists.

The historical trimmed deployment package reported zero production and nine development advisories, including one critical; this does not cover website/ZK dependencies or constitute independent audit. The later annual-burn candidate has separate local-EVM tests, not included in those historical counts. It is unaudited and undeployed officially. One TIME per net person and consecutive years are enforced in the candidate, but statistics authenticity still depends on administrator checking.

08 / DELIVERY PATH: Advance by conditions, not guaranteed dates.

Next decisions include first data year, baseline population and custody. The candidate locally validates the fixed 1.4 billion supply, burn permissions, reserve shortfalls and annual replay prevention. Data corrections, public execution and independent review remain to be completed alongside product requirements and utility.

Formal issuance also requires real entity/team disclosures, independent legal/security review, wallet deployment/funding/vesting acceptance on a public testnet, source verification and treasury-control rehearsal. A DEX needs actual paired assets and liquidity; each CEX reviews independently. No listing date, price or market depth is promised.

09 / REVIEW MATERIALS: Versions, source and open questions.

This is research whitepaper v0.1, with policy content dated 2 November 2026. It records the confirmed 1.4 billion initial supply and one-person/one-TIME manual annual burn rule, while reserves and execution arrangements remain undecided. It is not fundraising material, a rights certificate or a return promise. Read historical briefs and engineering tests in their own dated contexts; this whitepaper and the TIME asset page describe the current design.

Reference source, test records, threat models and supply policy are available from the website resources. Anonymous issuance, recovery linkage, real biometric deduplication, independent operation and production security remain important open questions.

Sources and materials

2024 national statistics communiqué: https://www.stats.gov.cn/sj/zxfb/202502/t20250228_1958817.html

2025 national statistics communiqué: https://www.stats.gov.cn/sj/zxfb/202602/t20260228_1962662.html

Engineering verification: https://time-humanity-protocol.growndisco.chatgpt.site/verification.html

Threat model: https://time-humanity-protocol.growndisco.chatgpt.site/docs/threat-model.html

TIME asset policy: https://time-humanity-protocol.growndisco.chatgpt.site/token.html