

HUMONEY

A Peer-to-Peer Currency Indexed to Human Basal Metabolism

Self-stabilising · collateral-backed · apolitical

Specification v2.0 · June 2026 · Open Community Standard

Authored by Oleh Bezuhlyi

Companion to ProtoLedger Core v2.0

Released under Apache 2.0 — fork it, challenge it, build it.

What this is. Humoney is a complete protocol for a self-stabilising currency whose unit is one day of human basal metabolism. It is designed to be built from components already in production — over-collateralised vaults, decentralised price oracles, a non-discretionary stabilisation controller, and finalised post-quantum cryptography — and to deploy in three phases beginning on existing settlement infrastructure. This document describes the protocol as designed to operate, not a network already running. The one property the design manages but does not claim to have proven is maintenance of the metabolic peg through a simultaneous collateral crash and food-energy price spike; Section 11 sets out the layered defences and states the residual risk without varnish.

Abstract

We present Humoney, a currency that holds its value against the one cost no economy can escape: the energy a human body must expend to remain alive. Fiat depreciates at the discretion of its issuer; gold's own value drifts; Bitcoin solved issuance but not volatility; fiat-pegged stablecoins re-import the very monetary politics they were meant to escape; and inflation-indexed “flatcoins” peg to a consumer basket that is an arbitrary, drifting committee artefact. Humoney instead defines its unit as a fixed physical quantity — one Reference-Human Basal Day (RHBD), 1,700 kilocalories or 1.976 kilowatt-hours of basal metabolism — and holds that unit's purchasing power against the delivered cost of meeting it. One Humoney (HU) is minted only against over-collateralised reserves and is continuously redeemable for reserve value not less than the Metabolic Cost Index (MCI), the market price of making one RHBD functionally available. A non-discretionary controller and open mint-and-redeem arbitrage hold the market price to the index; an any-asset reserve carrying an energy- and food-linked leg backs it with collateral correlated to the indexed quantity itself; under-collateralised positions are liquidated, and a governance-and-backstop token (HMG) recapitalises the system of last resort. Settlement begins on existing high-assurance infrastructure and migrates to a sovereign post-quantum DAG-BFT chain. The result is money that is physical, universal, and apolitical, denominated in human time from the day down to the second, and buildable today.

Unit: Humoney (HU) — a fungible token, 18 decimals on-chain, displayed in human-days (HU), human-hours (HUH), human-minutes (HUM), human-seconds (HUS). **Backing:** an over-collateralised, any-asset Reserve indexed to the Metabolic Cost Index (MCI). **Governance & backstop:** the Humoney Governance token (HMG).

1. Introduction

Money is meant to be a stable measure of value, yet every unit in wide use is referenced to a moving point. Fiat is referenced to issuer discretion and loses purchasing power at the tolerated rate of inflation. Gold fails the test of an ideal money because its own exchange value is non-stationary. Bitcoin removed the issuer but left a unit too volatile to quote a week's groceries. The stablecoins that followed pegged to the dollar — solving volatility by surrendering the entire point, since a dollar-pegged token is the dollar's monetary policy wearing a new logo. The most recent answer, the inflation-indexed flatcoin, is the closest yet: it targets a basket of consumer goods rather than a single fiat unit. But the basket is chosen, weighted, and revised by a committee, and so the question “stable against what?” is answered, once again, by something contingent and political.

There is one answer that is not contingent. Every transaction, however far up the chain of abstraction, is ultimately made so that some human can consume; and the irreducible, non-discretionary floor of human consumption is basal metabolism — the energy a body expends merely to remain a functioning organism. That quantity is measurable, identical in physical terms for every human, and beyond the reach of any central bank. Humoney references the unit of money to it. The remainder of this paper specifies how a currency can be issued against that reference, held to it without discretionary policy, and settled on infrastructure that exists today.

2. System Overview

Humoney is six interacting parts. None is novel in isolation; their composition around a metabolic unit is.

Component	Function
HU (the unit)	The stable currency. Minted only against collateral; redeemable for reserve value $\geq$ the MCI.
Vaults	Over-collateralised positions in which users lock assets and draw HU, up to a collateral-class ratio.
The Reserve	Protocol-held, diversified backing, including an energy- and food-linked leg correlated with the MCI.
Metabolic Oracle	A decentralised network that prices the Metabolic Reference Basket and publishes the MCI.
The Stabiliser	Open mint/redeem arbitrage plus a non-discretionary redemption-rate controller holding price to index.
HMG	Governance token and recapitalisation backstop of last resort; absorbs shortfall by dilution.

2.1 Lifecycle of a Humoney

Mint. A user opens a Vault, locks collateral, and draws HU up to the collateral class's ratio, valued against the current MCI. The HU is newly issued and fully backed. **Circulate.** HU transfers peer-to-peer, shielded by default; only a nullifier, a commitment, an encrypted note, a validity proof, and a plaintext fee are recorded. **Hold.** Because the unit is indexed to basal metabolism, a balance preserves its command over obligate metabolic provisioning regardless of fiat inflation. **Redeem.** HU is returned to a Vault to release collateral, or exchanged through the Stabiliser at the prevailing index. **Liquidate.** If a Vault falls below its minimum ratio, it is auctioned and its debt retired (Section 7). At every step the system-wide invariant holds: $\text{HU outstanding} \times \text{MCI} \leq \text{Reserve value}$.

3. The Unit: Human Basal Metabolism

Basal metabolic rate varies across individuals by nearly a factor of two with mass, age, sex, and ambient temperature, so the protocol fixes a reference quantity, exactly as metrology once fixed the kilogram by a reference artefact. The Reference-Human Basal Metabolic Rate (RH-BMR) is set, as a permanent constitutional constant, at 1,700 kilocalories per day — the basal figure, the obligate expenditure at complete rest. One Humoney is defined as one Reference-Human Basal Day (RHBD) of that expenditure. With the thermochemical conversion $1 \text{ kcal} \equiv 4,184 \text{ J}$, the constant yields an exact denomination ladder quantised in human time:

Denomination	Definition	Energy	Monetary role
HU (human-day)	1 RHBD	$1,700 \text{ kcal} = 7.1128 \text{ MJ} = 1.976 \text{ kWh}$	Base unit of account (mean basal power 82.3 W).
HUH (human-hour)	$\text{HU} / 24$	$70.83 \text{ kcal} = 296.4 \text{ kJ} = 82.3 \text{ Wh}$	Principal transactional denomination.
HUM (human-minute)	$\text{HU} / 1,440$	$1.181 \text{ kcal} = 4.939 \text{ kJ}$	Retail quantum, quoted at point of sale.
HUS (human-second)	$\text{HU} / 86,400$	82.3 J	Settlement quantum for fees and micro-payments.

Thus $1 \text{ HU} = 24 \text{ HUH} = 1,440 \text{ HUM} = 86,400 \text{ HUS}$. On-chain the token carries eighteen decimals, so the human-second — about $1.16 \times 10^{-5} \text{ HU}$ — sits far inside the available precision; the human-time denominations are display conventions over a single integer balance. A numerical regularity falls out of the mean basal power of 82.3 W: one human-hour is 82.3 Wh and one human-second is 82.3 J, each denomination equalling the reference power in its own time base. The unit definition is pure physics and never moves; it is the fixed end of the system against which everything else is measured.

4. The Metabolic Cost Index and Oracle Network

The unit is defined in energy; its purchasing power is enforced in money. The bridge between them is the Metabolic Cost Index (MCI): the delivered market cost of the Functional Availability of one RHBD — the basal requirement rendered actually consumable at the point of human use, as edible dietary energy in fixed staple proportions plus the minimal ancillary energy to prepare and access it. This bundle is the Metabolic Reference Basket (MRB). Its composition is fixed like the kilogram's; only its priced value floats, and it is priced at published global reference prices so that HU is one global unit despite local price dispersion.

Measured at the point of consumption. The MCI prices delivered, consumable provision — roughly 1.98 kWh per day of dietary energy plus minimal ancillary energy — not the larger upstream primary energy of production, and not per-capita energy footprint. Restricting measurement to consumption is what keeps Humoney a basal-metabolic unit rather than a volatile industrial-energy index.

The MCI is produced by a decentralised oracle network rather than a single feed, because control of the index is control of the unit. Independent reporters submit priced observations of the fixed MRB; the protocol takes the median; the basket and the computation are published so any party can reproduce the

figure from raw public prices and challenge a deviant report. Circuit breakers bound the damage from manipulation or outage: if reporters diverge beyond a threshold or a feed goes stale, the index freezes at its last valid value and new minting tightens until the feed is restored. The oracle is the system's most valuable target, and is treated as such throughout the design.

5. Minting and Redemption: the Vault System

HU enters existence only through over-collateralised Vaults. A user locks collateral and may draw HU whose MCI-denominated value is at most the locked value divided by the collateral class's minimum ratio. Drawn HU accrues a stability fee — a small ongoing charge that funds the surplus buffer (Section 7) — and the Vault may be topped up, partially repaid, or closed at any time by returning the HU drawn. Collateral is unrestricted in kind but tiered by risk:

Collateral class	Min. ratio	Liq. penalty	Reserve role
Blue-chip crypto (BTC, ETH-class)	150%	13%	Core volatile backing.
Tokenised short-dated sovereign debt	110%	6%	Low-volatility ballast.
Tokenised energy & dietary commodities	130%	10%	The metabolic-linked leg.

The third class is the design's distinguishing feature, available only to a metabolically-defined unit. Because HU denominates a fixed energy quantity, the Reserve can hold energy- and dietary-commodity-linked claims — collateral correlated with the very quantity the MCI tracks. A rise in food or energy prices that lifts the MCI also lifts the value of the leg backing it, so the reserve tends to strengthen exactly when the obligation it must meet grows. The correlation is partial, not perfect, and the leg's share of the Reserve is a governable band (initially targeted at one fifth to two fifths). System-wide over-collateralisation is maintained above the sum of the per-class minima and widened automatically under stress, so the continuous invariant — $\text{HU outstanding} \times \text{MCI} \leq \text{Reserve value, with margin}$ — holds with room to spare.

6. Stabilisation

Two mechanisms hold the market price of HU to the MCI, neither of which requires a committee to set a rate. The first is open arbitrage: anyone may mint HU by locking collateral and redeem HU for collateral at the prevailing index, so a market price above the index invites new minting and selling, and a price below it invites buying and redemption, each force pushing price back toward index.

The second is a non-discretionary redemption-rate controller, of the kind proven by the RAI reflexer asset. Let the error be the fractional deviation of market price from index, $e = (P_{\text{market}} - \text{MCI}) / \text{MCI}$. The controller sets a redemption rate

$$r = - (K_p \cdot e + K_i \cdot \int e \, dt + K_d \cdot de/dt)$$

applied continuously to the redemption value of HU. When HU trades persistently above the index, the rate turns negative, gently reducing the reward for holding and increasing the incentive to mint and sell, which lowers price; when it trades below, the rate turns positive and the incentives reverse. The controller damps deviations without anyone deciding a target by fiat — the index is set by physics and the market, and the gains are governable parameters, not monetary policy. There is no uncollateralised issuance and no algorithmic seigniorage; capital efficiency is deliberately traded for solvency.

Optional metabolic demurrage. Because basal expenditure is continuous — the reference human dissipates 82.3 W whether or not money moves — the protocol may levy a small carrying charge on idle balances, recirculated to active holders or the commons, to discourage hoarding. The rate is a governance parameter calibrated to circulation, not the physiological burn rate. It is disabled by default.

7. Liquidation and the Backstop

If collateral falls so that a Vault breaches its minimum ratio, the Vault is liquidated: its collateral is auctioned for HU, the drawn HU is burned to retire the debt, and the liquidation penalty is added to the surplus buffer. Auctions are permissionless, so liquidation capacity scales with the market rather than with any privileged keeper.

Three reserves of strength stand behind the peg, drawn upon in order. **First**, per-Vault over-collateralisation absorbs ordinary price moves. **Second**, the surplus buffer — accumulated stability fees and penalties — absorbs liquidation shortfalls before any holder is touched. **Third**, if a violent, correlated drawdown drives the system below full backing despite the first two, HMG is minted and sold to recapitalise, diluting governance holders rather than HU holders. This is the proven debt-auction backstop of mature collateralised-stablecoin systems, and it aligns the people who govern the parameters with the people who bear the tail risk of getting them wrong.

8. Settlement, Cryptography, and Privacy

Humoney's value does not depend on owning a chain, so it ships on the best available rails and earns sovereignty later. In its first phase the protocol is a set of audited contracts on an established, high-assurance, low-fee settlement layer, inheriting that layer's security and liquidity from day one. In its second phase settlement migrates to a sovereign ProtoLedger-Core-class Layer 1: a DAG-BFT consensus backbone with sub-second deterministic finality, post-quantum from genesis, and private by default. Signatures use ML-DSA (FIPS 204) as a mandatory baseline with algorithm agility, so the scheme is a governable parameter rather than a permanent bet; key encapsulation uses ML-KEM-768 (FIPS 203); proofs use Circle STARKs, which need no trusted setup and rest on hash hardness rather than elliptic curves. Falcon / FN-DSA is admitted as an optional compact scheme once FIPS 206 is finalised. Every transfer is shielded by default — amounts as commitments, validity by STARK proof — with user-issued viewing keys and compliance proofs for selective, revocable disclosure, never a protocol backdoor.

9. Governance

Every tunable parameter lives on-chain and changes only when voting conditions are met; there is no foundation key and no upgrade dictator. HMG carries the vote, weighted to blunt plutocratic capture, and the parameters that define the unit itself are walled off at the highest threshold, because they are the meaning of every HU in existence.

Proposal type	Threshold	Notice	Scope
Risk parameter	51%	4 days	Collateral ratios, stability fees, controller gains, reserve bands.
Protocol upgrade	66.7%	30 days	Contract or consensus changes.
Emergency action	75%	24 hours	Pause minting, oracle circuit-breaker override; requires auditor co-signature.
Constitutional amendment	80%	180 days	The RH-BMR constant and the Metabolic Reference Basket composition.

10. The Human Dividend (optional)

Because Humoney's unit is literally a day of human metabolism, the protocol admits a clean, optional distribution layer that the early phases neither require nor depend upon. Once a privacy-preserving proof-of-personhood network is live, a per-verified-human dividend may be paid in HU from protocol surplus or a distinct distribution stream — never by minting HU outside the collateral invariant. The dividend's size is non-arbitrary by construction: a grant of a small integer number of HU is, precisely, that many days of basal metabolic provisioning. Uniqueness relies on World-ID-class proofs — an iris reduced on-device to a template and then to a zero-knowledge proof of uniqueness, with no biometric ever leaving the holder's device. This layer is deliberately isolated from the peg: its unsolved problems — enrolment integrity, coercion and credential rental, and registry centralisation — must never be load-bearing for the currency's value, and here they are not.

11. Security and Failure Modes

Oracle capture. Control of the MCI is control of the unit. The defence is plural reporting with a median, a publicly reproducible basket so any observer can falsify a bad print, and circuit breakers that freeze the index and tighten minting on divergence or staleness. This raises the cost of capture sharply but does not reduce it to zero; oracle decentralisation is a permanent area of hardening, not a solved checkbox.

Collateral risk and the central failure mode. The honest worst case for any collateral-backed money is a violent, correlated drawdown — and for Humoney it has a specific shape: a systemic event that depresses collateral while simultaneously spiking food and energy prices raises the MCI at the very moment the Reserve is worth least. Four layers stand against it: over-collateralisation, the surplus buffer, the HMG recapitalisation backstop, and the metabolic-linked Reserve leg, whose value rises with the same prices that raise the index. The leg is what makes Humoney structurally better-defended here than a fiat- or basket-pegged design, because part of its backing moves with its obligation. It is a partial hedge, not a guarantee.

Stated plainly: no collateral-backed currency, Humoney included, has been proven to hold its peg through a 2008- or Terra-scale correlated event, and Humoney makes no claim to have done so. This is the property the whole architecture is built to manage, and it is the property that must be demonstrated by adversarial economic simulation and independent audit — before, not after, the peg is offered to users as dependable. Everything else in this paper is engineering that exists; this is the engineering that must be proven.

Governance and custody. The Metabolic Reference Basket and RH-BMR constant are the system's highest-value attack target, which is why their amendment sits behind the longest notice and highest threshold in the protocol. Real-world-asset and commodity legs add custodial and legal-recourse surface that pure crypto collateral does not; these dependencies are named, sized, and governed rather than assumed away.

12. Deployment Roadmap

Phase	Scope	Settlement	Status
1	HU, Vaults, Metabolic Oracle, Stabiliser, HMG, liquidation, surplus buffer	Existing high-assurance L2	Mainnet target
2	Sovereign migration: DAG-BFT finality, post-quantum from genesis, default privacy	ProtoLedger-class L1	Planned

Phase	Scope	Settlement	Status
3	Human Dividend via proof-of-personhood; one-person governance weighting	—	Research

The phases are independent by design. Phase 1 delivers a working metabolic currency on infrastructure that exists today; Phase 2 buys sovereignty and forward security without changing the unit; Phase 3 adds an egalitarian distribution that the currency never depends upon. No phase blocks the one before it — the mistake of bolting a whole system to a component that does not yet exist is not repeated here.

13. Conclusion

Humoney answers the oldest open question in monetary design — stable against what? — with the only answer that is not a matter of opinion: stable against the energy a human must spend to live. It issues that money against real collateral, holds it to the index without discretionary policy, defends it with reserves that move with the obligation they secure, and settles it on rails that exist now. It does not need a new consensus breakthrough, a token sale, or a leap of faith in untested cryptography; it needs careful engineering of parts already in production and honest proof of the one property — peg survival through a correlated crash — that no collateral-backed money has yet demonstrated. The unit is not worth one dollar, and not worth one arbitrary basket. It is worth one day of human life, measured in joules, and quantised down to the second.

Fork it, challenge it, build it.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] J. F. Nash, “Ideal Money” and “Asymptotically Ideal Money,” 1995–2008.
[3] F. Soddy, “Wealth, Virtual Wealth and Debt,” 1926; Technocracy Inc., energy-certificate proposals, 1930s.
[4] Reflexer, “RAI: a non-pegged, controller-stabilised reflexer asset.”
[5] Laguna Labs, “Nuon,” and Truflation index; Frax, “Frax Price Index.”
[6] MakerDAO, “The Dai Stablecoin System” (collateralised vaults, debt-auction backstop).
[7] Tools for Humanity, “World ID” proof of personhood (iris → zero-knowledge uniqueness).
[8] NIST, FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA), Aug 2024; FIPS 206 (FN-DSA) — draft.
[9] StarkWare, “Circle STARKs,” 2024.
[10] Danezis et al., “Narwhal & Tusk”; Spiegelman et al., “Bullshark”; Arun et al., “Shoal++.”
[11] O. Bezuhlyi, “ProtoLedger Core v2.0,” 2026.

Locked constants. RH-BMR $\equiv$ 1,700 kcal/day (constitutional, permanent). 1 kcal $\equiv$ 4,184 J. 1 HU $\equiv$ 1 RHBD = 1,700 kcal = 7.1128 MJ = 1.976 kWh (mean basal power 82.3 W). 1 HUH = HU/24 = 70.83 kcal = 296.4 kJ = 82.3 Wh. 1 HUM = HU/1,440 = 1.181 kcal = 4.939 kJ. 1 HUS = HU/86,400 = 82.3 J. 1 HU = 24 HUH = 1,440 HUM = 86,400 HUS. On-chain precision: 18 decimals.