

1 Axioms of U_1 Monetary Systems

Axiom 1 (A_1 Energy-Bounded Leader Election). *Block production requires verifiable expenditure of physical energy such that issuance cost $E_{\text{issue}} \geq E_{\text{verify}}$. No valid unit may exist without irreversible work.*

Axiom 2 (A_2 Public Verifiability). *Any observer with public data and bounded computation can audit total supply, validate transaction history, and verify current state without trusted intermediaries.*

Axiom 3 (A_3 Probabilistic Finality). *The ledger exhibits irreversible settlement with known probabilistic bounds; reorganization probability decays exponentially with confirmation depth under the honest-majority assumption.*

Axiom 4 (A_4 Monetary Closure). *Aggregate monetary supply is finite and mathematically enforced: $\sum U_t \leq S_{\text{max}}$ across all valid histories. Inflationary creation is invalid under consensus rules.*

2 Coordination Capacity

This section formalizes the notion of *coordination capacity* for open, adversarial monetary systems, isolates irreversibility as the primitive resource, and states the U_1 Coordination Capacity Conjecture.

2.1 Irreversibility as the Primitive

Definition 1 (Irreversible Work Step). A work step is *irreversible* if its physical realization increases entropy in the environment such that no observer with bounded resources can algorithmically reconstruct a pre-image of the microscopic state prior to the step.

We write $E_{\text{irr}} > 0$ for the minimal energy cost of such a step at a given ambient temperature.

Definition 2 (Physics-Anchored Protocol). A protocol Π is *physics-anchored* if every admissible block production event must include at least one irreversible work step whose successful completion is:

1. publicly and efficiently verifiable, and
2. infeasible to simulate without incurring comparable physical energy cost.

In other words, physics-anchored protocols encode consensus progress into the irreversibility of the underlying physical process (e.g. PoW), rather than into institutional decree or access-controlled identities.

2.2 Atomic Unit of Account

Definition 3 (Atomic Unit of Account). Let Π be a physics-anchored monetary protocol with total supply process $(U_t)_{t \geq 0}$.

An *atomic unit of account* U is the smallest denomination such that:

1. (Indivisibility) No valid ledger state can represent a claim smaller than U .
2. (Fungibility) Any two claims of size U are mutually substitutable under the protocol's transfer rules.
3. (Monetary Closure) The aggregate supply satisfies $\sum U_t \leq S_{\max}$ across all valid histories.
4. (Settlement Granularity) Every irreversible settlement event can be decomposed into a finite change in the allocation of atomic units U .

Remark 1. In Bitcoin, the atomic unit is $U = 1$ satoshi and $S_{\max} = 21 \times 10^6 \text{ BTC} = 2.1 \times 10^{15}$ satoshis. For any protocol satisfying A_4 (Monetary Closure), an analogous U exists.

2.3 Coordination Flow and Capacity

We now formalize coordination as an information flow from latent economic reality into a publicly settled ledger.

Definition 4 (Economic State and Ledger State). Let $(\Theta_t)_{t \geq 0}$ denote a (possibly high-dimensional) stochastic process capturing the true economic preferences and claims of agents at time t , and let $(A_t)_{t \geq 0}$ denote the publicly settled ledger state produced by protocol Π at time t .

Both processes are defined on a common probability space, and (A_t) is adapted to the filtration generated by protocol-visible messages and blocks.

Definition 5 (Coordination Flow). For a fixed protocol Π , the *coordination flow rate* is

$$\dot{V}_{\text{coord}}(\Pi) = \lim_{T \rightarrow \infty} \frac{1}{T} I(\Theta_{0:T}; A_{0:T}),$$

whenever the limit exists, where $I(\cdot; \cdot)$ denotes mutual information.

Intuitively, $\dot{V}_{\text{coord}}(\Pi)$ measures how many bits of true economic intent are irreversibly compressed into the public ledger per unit time.

Definition 6 (Coordination Capacity). Let $\mathcal{M}_{\text{phys}}$ denote the class of physics-anchored protocols satisfying:

1. public verifiability (A_2),
2. open participation (permissionless entry and exit),
3. bounded adversary resources (e.g. an honest-majority work budget),

4. physically irreversible settlement cost (A_1).

The *coordination capacity* of the environment is

$$C_{\text{coord}} = \sup_{\Pi \in \mathcal{M}_{\text{phys}}} \dot{V}_{\text{coord}}(\Pi) = \sup_{\Pi \in \mathcal{M}_{\text{phys}}} \lim_{T \rightarrow \infty} \frac{1}{T} I(\Theta_{0:T}; A_{0:T}).$$

Thus C_{coord} is to adversarial economic settlement what Shannon capacity is to communication over noisy channels: the maximal information rate at which true economic state can be mapped into a canonical public ledger with arbitrarily small corruption probability, under fixed physical and adversarial constraints.

2.4 Security Exponent and Irreversibility Density

We now connect settlement reliability to the rate of irreversible work performed by honest participants.

Definition 7 (Security Exponent). Consider a physics-anchored protocol Π exhibiting probabilistic finality (A_3). For a reorganization depth parameter $k \in \mathbb{N}$, let

$$P_{\text{reorg}}(k) = \Pr(\text{ledger reorganization of depth} \geq k).$$

If there exists $\beta > 0$ and k_0 such that

$$P_{\text{reorg}}(k) \leq \exp(-\beta k) \quad \text{for all } k \geq k_0,$$

we say that Π has *security exponent* β .

Definition 8 (Irreversibility Density). Let \dot{E}_{honest} denote the long-run honest irreversible work rate (in joules per second) invested in maintaining consensus for Π , and let \dot{U}_{secured} denote the long-run rate (in units per second) at which atomic units U are involved in economically meaningful settled transfers.

The *irreversibility density* of Π is

$$\rho_{\text{irr}}(\Pi) = \frac{\dot{E}_{\text{honest}}}{\dot{U}_{\text{secured}}} \quad \text{with units} \quad \frac{\text{J}}{\text{U}}.$$

Remark 2. Heuristically, ρ_{irr} can be interpreted as the average amount of physically irreversible work crystallized into the ledger per unit of account. Systems with $\rho_{\text{irr}} \rightarrow 0$ cannot maintain a meaningful barrier against adversarial rewriting of history in an open, permissionless setting.

In PoW-style U_1 systems, empirical and theoretical arguments suggest that, under competitive mining and difficulty adjustment (T_1 , T_2), there exists a protocol-dependent constant $c > 0$ such that

$$\beta(\Pi) \approx c \cdot \frac{\dot{E}_{\text{honest}}}{V_{\text{secured}}},$$

where V_{secured} is the total economic value (e.g. in units U times purchasing power) that depends on Π for settlement.¹

¹The precise choice of V_{secured} (e.g. fee-paying volume, non-churn flow, or broader balance

2.5 Model Boundary: Physics vs. Coercion

The above definitions explicitly restrict attention to *physics-anchored* protocols in $\mathcal{M}_{\text{phys}}$.

Definition 9 (Institution-Anchored Ledger). A ledger Π_{inst} is *institution-anchored* if irreversibility of entries is enforced primarily by:

1. legal decree or administrative authority,
2. access-controlled identities or whitelists,
3. coercive enforcement (e.g. courts, police, capital controls),

rather than by publicly verifiable irreversible work steps.

Fiat currencies, bank databases, and permissioned ledgers typically fall into this class: they may exhibit practical irreversibility within a jurisdiction, but it is not rooted in physics and is not permissionless or globally auditable in the sense of A_1 – A_4 .

Remark 3. Coordination capacity C_{coord} is defined only over $\mathcal{M}_{\text{phys}}$. Institution-anchored systems may coordinate agents via coercive trust hierarchies, but they do not approach a physics-limited capacity in the Shannon sense, and they do not provide irreversibility that is independent of specific institutional arrangements.

2.6 U_1 Coordination Capacity Conjecture

We can now restate the core conjecture in this refined language.

Conjecture 5 (U_1 Coordination Capacity Conjecture). *Consider the class $\mathcal{M}_{\text{phys}}$ of physics-anchored protocols operating in an open, permissionless, adversarial environment with a bounded-work attacker (honest-majority assumption).*

Then:

1. *A protocol $\Pi \in \mathcal{M}_{\text{phys}}$ achieves strictly positive coordination capacity ($\dot{V}_{\text{coord}}(\Pi) > 0$) if and only if it satisfies the U_1 axioms: A_1 (energy-bounded issuance), A_2 (public verifiability), A_3 (probabilistic finality), A_4 (monetary closure).*
2. *For any such Π with adversary work fraction $q < p$ (honest fraction p), there exists $\beta(\Pi) > 0$ such that the reorganization probability obeys an exponential bound*

$$\Pr(\text{reorg depth} \geq k) \leq \left(\frac{q}{p}\right)^k = \exp(-\beta(\Pi) k) \quad \text{for all sufficiently large } k.$$

at risk) is an empirical modeling decision. For the purposes of the conjecture, it suffices that V_{secured} captures the value whose coordination depends critically on Π .

3. Among protocols satisfying A_1 – A_4 , U_1 -style PoW monetary systems can achieve security exponents $\beta(\Pi)$ arbitrarily close to the physical limit imposed by their irreversibility density:

$$\beta(\Pi) \lesssim c \cdot \frac{\dot{E}_{\text{honest}}}{V_{\text{secured}}},$$

for some protocol- and environment-dependent constant $c > 0$, with equality approached in the limit of optimal encoding of economic state into ledger state.

Corollary 6 (Vanishing Irreversibility Density). *Within $\mathcal{M}_{\text{phys}}$, any family of protocols $(\Pi_n)_{n \in \mathbb{N}}$ with irreversibility density $\rho_{\text{irr}}(\Pi_n) \rightarrow 0$ as $n \rightarrow \infty$ satisfies*

$$\lim_{n \rightarrow \infty} \dot{V}_{\text{coord}}(\Pi_n) = 0.$$

In particular, physics-anchored systems whose marginal unit of account is not backed by a nontrivial amount of irreversible work cannot achieve nonzero coordination capacity in the limit.

The conjecture thus states that U_1 systems are to economic coordination what Shannon-capacity-achieving codes are to communication: they saturate a physically imposed limit on reliable performance in a noisy, adversarial universe.

2.7 Dual-Entropy Characterization

We now introduce a dimensionless measure that unifies thermodynamic irreversibility with informational predictability. This characterization provides a scalar invariant that captures the essential tension in monetary coordination: certainty about the past versus uncertainty about the future.

2.7.1 Thermodynamic Irreversibility

Definition 10 (Thermodynamic Irreversibility (Bit-Normalized)). For a physics-anchored protocol Π with cumulative irreversible energy expenditure $E_{\text{cum}}(t)$ up to time t , define the *thermodynamic irreversibility* (in bits) as

$$\mathcal{S}_{\Pi}(t) = \frac{E_{\text{cum}}(t)}{k_B T \ln 2},$$

where $k_B \approx 1.38 \times 10^{-23}$ J/K is Boltzmann’s constant, T is ambient temperature (typically ≈ 300 K), and $k_B T \ln 2 \approx 2.87 \times 10^{-21}$ J is the Landauer energy cost per bit of erasure.

Remark 4. \mathcal{S}_{Π} counts the number of bits whose erasure would require energy equal to the cumulative work invested in Π . This provides a physics-grounded measure of how “deep” the protocol’s history is anchored in thermodynamic irreversibility. The Landauer normalization ensures \mathcal{S} has units of bits, enabling direct comparison with informational entropy.

Remark 5 (Connection to Landauer’s Principle). Landauer’s principle (1961) establishes that erasing one bit of information requires dissipating at least $k_B T \ln 2$ joules of energy as heat. By normalizing cumulative work by this quantity, \mathcal{S}_Π measures the thermodynamic “depth” of the ledger in fundamental physical units.

2.7.2 Monetary Informational Entropy

Definition 11 (Monetary Informational Entropy). For a monetary protocol Π with supply process $(U_t)_{t \geq 0}$ and policy state $(\theta_t)_{t \geq 0}$, define the *monetary informational entropy* at horizon $\tau > 0$ as

$$\mathcal{H}_\Pi(\tau) = H(\text{MonetaryState}_{t+\tau} \mid \text{MonetaryState}_t, \text{Protocol}_t),$$

where $H(\cdot \mid \cdot)$ denotes conditional Shannon entropy (in bits), and MonetaryState encompasses:

- total supply U_t ,
- issuance rate \dot{U}_t ,
- policy parameters (inflation targets, governance rules),
- any state variables affecting future monetary outcomes.

Remark 6. $\mathcal{H}_\Pi(\tau)$ measures the irreducible uncertainty (in bits) about the monetary system’s future state at horizon τ , given complete knowledge of its current state and rules. For protocols with deterministic supply schedules and ossified rule sets, $\mathcal{H}_\Pi(\tau) \rightarrow 0$ for all τ .

Remark 7 (Orthogonality of \mathcal{S} and \mathcal{H}). These two quantities are logically independent:

- \mathcal{S} measures *how hard it is to change the past* (thermodynamic irreversibility).
- \mathcal{H} measures *how hard it is to predict the future* (informational uncertainty).

A system can have any combination: high \mathcal{S} with high \mathcal{H} (irreversible but unpredictable), low \mathcal{S} with low \mathcal{H} (reversible but predictable), etc.

2.7.3 The Coordination Capacity Ratio

Definition 12 (Coordination Capacity Ratio). The *coordination capacity ratio* of protocol Π is

$$\kappa_\Pi \equiv \frac{\mathcal{S}_\Pi}{\mathcal{H}_\Pi}$$

with units: bits/bits = dimensionless.

κ_Π measures the ratio of thermodynamic commitment (secured past) to monetary uncertainty (unknown future):

$$\kappa = \frac{\text{Irreversibility}}{\text{Uncertainty}} = \frac{\text{What cannot be undone}}{\text{What cannot be known}}.$$

High κ indicates a system with strong irreversibility and high predictability—the optimal configuration for coordination.

Remark 8 (Analogy to Fundamental Dimensionless Ratios). The ratio $\kappa = \mathcal{S}/\mathcal{H}$ is structurally analogous to other fundamental dimensionless quantities in physics:

Ratio	Formula	Tension
Reynolds number	$Re = \rho v L / \mu$	Inertia vs. viscosity
Signal-to-noise	$SNR = P_s / P_n$	Signal vs. noise
Carnot efficiency	$\eta = 1 - T_C / T_H$	Cold vs. hot reservoir
Coordination capacity	$\kappa = \mathcal{S} / \mathcal{H}$	Irreversibility vs. uncertainty

2.7.4 Properties of κ

[Boundary Behavior] For any physics-anchored protocol Π :

1. If $\mathcal{S}_\Pi \rightarrow \infty$ and $\mathcal{H}_\Pi \rightarrow 0^+$, then $\kappa_\Pi \rightarrow \infty$.
2. If $\mathcal{S}_\Pi \rightarrow 0$ (no thermodynamic anchoring), then $\kappa_\Pi \rightarrow 0$ regardless of \mathcal{H}_Π .
3. If $\mathcal{H}_\Pi \rightarrow \infty$ (unbounded policy uncertainty), then $\kappa_\Pi \rightarrow 0$ regardless of \mathcal{S}_Π .

Proof. Direct from the definition $\kappa = \mathcal{S}/\mathcal{H}$ and properties of limits. \square

Corollary 7 (Optimal Coordination Regime). *Maximum coordination capacity is achieved in the regime:*

$$\mathcal{S} \rightarrow \infty, \quad \mathcal{H} \rightarrow 0 \quad \implies \quad \kappa \rightarrow \infty.$$

This corresponds to a protocol with maximal thermodynamic security and minimal monetary uncertainty.

2.7.5 Capital Flow Conjecture

Conjecture 8 (Capital Flow Gradient). *Let Π_A and Π_B be competing monetary protocols with coordination capacity ratios κ_A and κ_B respectively.*

If $\kappa_B > \kappa_A$, then in the long run, capital flows from Π_A to Π_B at a rate proportional to the gradient:

$$\dot{K}_{A \rightarrow B} \propto (\kappa_B - \kappa_A) \cdot K_A,$$

where K_A is capital denominated in system A .

Remark 9. This conjecture formalizes the intuition that capital flows “downhill” in entropy space, analogous to:

- heat flow down temperature gradients (thermodynamics),
- mass flow down gravitational potentials (mechanics),
- current flow down voltage differentials (electromagnetism).

The coordination capacity differential $\Delta\kappa = \kappa_B - \kappa_A$ acts as the “potential gradient” driving capital migration.

2.7.6 Empirical Estimates

We now apply the framework to three monetary systems.

[Bitcoin] For Bitcoin as of 2025:

- Cumulative PoW energy: $E_{\text{cum}} \approx 2.7 \times 10^{18}$ J (estimated 750 TWh total since 2009).
- At $T = 300$ K:

$$\mathcal{S}_{\text{BTC}} = \frac{2.7 \times 10^{18}}{2.87 \times 10^{-21}} \approx 10^{39} \text{ bits.}$$

- Supply uncertainty: $\mathcal{H}_{\text{BTC}} \approx 1$ bit (deterministic halving schedule, protocol ossification, Schelling point against rule changes).
- Coordination capacity ratio: $\kappa_{\text{BTC}} \approx 10^{39}$.

[Gold] For gold as a monetary system:

- Physical extraction energy provides atomic verification ($\sim 10^{19}$ – 10^{20} bits equivalent) but does not secure the ownership ledger.
- Ownership record is institution-anchored (vulnerable to confiscation, re-hypothecation, paper claims).
- Effective thermodynamic irreversibility of the *monetary* system: $\mathcal{S}_{\text{Gold}} \approx 10^{19}$ – 10^{20} bits (physical verification only).
- Policy uncertainty (confiscation risk, paper-to-physical ratio, export controls): $\mathcal{H}_{\text{Gold}} \approx 10$ bits.
- Coordination capacity ratio: $\kappa_{\text{Gold}} \approx 10^{18}$ – 10^{19} .

[Fiat Currency (USD)] For the US dollar:

- No thermodynamic anchoring of the ledger (database entries, editable by administrative action): $\mathcal{S}_{\text{USD}} \approx 0$.
- High policy uncertainty (M2 growth unpredictable, inflation targets adjustable, fiscal policy volatile, CBDC transition): $\mathcal{H}_{\text{USD}} \approx 20$ bits.

- Coordination capacity ratio: $\kappa_{\text{USD}} \approx 0$.

Corollary 9 (Hierarchy of Coordination Capacity). *Under the above estimates:*

$$\kappa_{\text{BTC}} \gg \kappa_{\text{Gold}} \gg \kappa_{\text{USD}}.$$

Quantitatively:

$$\begin{aligned}\kappa_{\text{BTC}}/\kappa_{\text{Gold}} &\approx 10^{20}, \\ \kappa_{\text{Gold}}/\kappa_{\text{USD}} &\approx 10^{18}\text{--}10^{19}.\end{aligned}$$

The ratio $\kappa_{\text{BTC}}/\kappa_{\text{Gold}} \approx 10^{20}$ suggests Bitcoin represents a qualitative phase transition in coordination capacity, not merely an incremental improvement over prior monetary technologies.

2.7.7 Relation to Prior Definitions

The coordination capacity ratio κ complements the earlier definitions in this section:

- **Irreversibility density** ρ_{irr} (Definition 4.X) measures joules per unit transferred—a flow quantity.
- **Security exponent** β (Definition 4.X) measures the exponential decay rate of reorganization probability.
- **Coordination capacity ratio** κ measures the ratio of cumulative thermodynamic depth to monetary uncertainty—a stock quantity capturing the system’s attractiveness as a coordination substrate.

These quantities are related: high ρ_{irr} contributes to high \mathcal{S} (cumulative irreversibility), while protocol ossification contributes to low \mathcal{H} (monetary predictability). Together, they determine κ .

Remark 10 (Why κ Matters). While C_{coord} , ρ_{irr} , and β characterize the *operational* properties of a protocol (capacity, density, security), κ characterizes its *attractiveness* as a coordination substrate. The Capital Flow Conjecture (Conjecture ??) posits that κ determines long-run capital allocation across competing monetary systems.

3 Derived Theorems

Theorem 10 (T_1 Homeostatic Convergence). *In a competitive mining market obeying A_1 and A_3 , price–cost deviations are punished by market dynamics; expected divergence is mean-reverting.*

Theorem 11 (T_2 Security Scaling). *Given A_1 and open entry, sustainable security expenditure grows as an increasing function of civilization’s accessible energy E_{civ} .*