Celaya Chain Protocol: A Layer 3 Blockchain Architecture for Coherence-Based Governance

Whitepaper v1.0

Christopher Celaya
Celaya Solutions, El Paso, Texas
hello@celayasolutions.com

February 22, 2026

Technical Report CS:CCSIP-2026-001

Abstract

Celaya Chain Protocol (CCP) proposes a Layer 3 blockchain architecture, extending the programmable logic of Layer 2 systems with a layer designed to evaluate judgment. Where Layer 1 stores value and Layer 2 programs value, CCP governs the conditions under which value is legitimate. This is achieved through three proposed primitives: SAFE, a multi-dimensional reputation vector intended to make trust resistant to single-axis manipulation; Proof of Coherence, a consensus framework that validates actors across identity, reputation, policy, action, and biological continuity simultaneously; and a living constitutional governance layer in which no rule is permanent and founding authority dilutes mathematically as the network grows. CCP makes a single claim: coherence should determine authority. Everything else follows from that.

Keywords: blockchain; Layer 3 protocol; coherence governance; multi-dimensional reputation; biological identity; Proof of Coherence; decentralized autonomous organization; Sybil resistance; living constitution; authority decay

1. INTRODUCTION: WHY RULES WITHOUT JUDGMENT ARE INSUFFICIENT

Bitcoin solved trustless settlement between strangers [1]. Ethereum extended this with programmable logic [2]. Both assume that correct execution of rules is sufficient for coordination. CCP begins from a different assumption: rules without judgment are incomplete. A system that executes correctly but cannot reason about whether it should, and cannot distinguish a coherent actor from a sophisticated adversary, is not ready for the coordination problems civilization actually faces.

The blockchain trilemma, commonly described as the tension among security, scalability, and decentralization, has shaped every major L1 and L2 protocol built to date. Bitcoin prioritizes security and decentralization at the cost of throughput. Ethereum extends programmable execution while navigating its own decentralization and scaling tradeoffs. Solana prioritizes speed and throughput while accepting a different security and decentralization profile. Every choice encodes a tradeoff at genesis, then asks governance to live inside it.

CCP introduces a fourth variable the trilemma does not account for: adaptability. Not as a fourth point competing with the other three, but as a control layer governing the ratios between them. A living

constitutional governance system can reconfigure its own tradeoffs as conditions change. The trilemma describes a static space. CCP proposes a way to move through that space.

Layer 1 stores truth. Layer 2 programs truth. Layer 3 governs the conditions under which truth is legitimate. This requires judgment: the capacity to evaluate not just whether an action followed the rules, but whether the actor has demonstrated the coherence to be trusted with authority in the first place. To CCP's knowledge, no deployed blockchain protocol treats this question as a first-class governance layer. CCP is built around it.

The authority equation is not just mathematics. It is an ethical claim expressed in formal language.

2. THE SAFE LAYER: MAKING TRUST UNGAMEABLE

Every existing reputation system makes the same mistake. It collapses trust into a single dimension. Credit scores reduce financial behavior to one number. Star ratings reduce service quality to one number. Follower counts reduce influence to one number. Single-axis systems are not just incomplete: they are actively dangerous.

A single-axis reputation score creates a direct incentive toward gaming. If one number determines access, every rational actor will optimize that number. The optimization itself degrades the metric's meaning. This is Goodhart's Law applied to trust infrastructure, and it has distorted many reputation systems built to date [6].

CCP introduces SAFE: a multi-dimensional reputation vector in which no single axis can dominate. An actor must demonstrate sustained performance across five independent dimensions simultaneously:

Identity Verification (I): The depth and continuity of proven identity, from anonymous public keys through full biological verification.

Reputation Score (R): Historical behavior composite across all network interactions, weighted by recency and severity.

Policy Compliance (P): Ratio of actions that respected governance constraints versus those that were flagged, disputed, or reversed.

Action Audit Score (X): Granular evaluation of specific actions: transactions, votes, proposals, delegations. Each action is scored independently.

Biological Continuity (B): Continuous proof that the actor is a living, present human. Not a static check but a sequential, verifiable chain of biological presence.

The composite score is a weighted geometric mean, designed to resist single-axis manipulation:

$$C(t) = \left(I^{\beta} \cdot R^{\gamma} \cdot P^{\delta} \cdot X^{\varepsilon} \cdot B^{\zeta} \right)^{1/(\beta+\gamma+\delta+\varepsilon+\zeta)} \quad (1)$$

All weights (β, γ, δ, ε, ζ) are governed by the living constitution. The DAO owns every parameter. As the network matures and learns what coherence actually looks like in practice, the weights adapt. SAFE is not a fixed scoring system. It is a living measurement of demonstrated alignment.

Trust in CCP is not assigned. It is not inherited. It is not purchased. It is earned, across five independent dimensions, and continuously verified against the immutable record of what an actor has actually done.

3. BIOLOGICAL IDENTITY: THE LAYER DESIGNED TO RESIST FORGERY

Most digital identity systems share a fundamental vulnerability: the entity presenting credentials and the entity that earned them can be different. Passwords are stolen. Keys are compromised.

Accounts are hijacked. The credential proves the possession of a secret, not the presence of a person. This distinction has been tolerable for low-stakes systems. It becomes catastrophic when identity determines authority over critical infrastructure, medical decisions, or governance of systems that affect human lives.

CCP introduces biological identity as a protocol primitive. Not as an authentication layer sitting above the protocol, but as a first-class participant in consensus itself.

The foundation is Proof of Existence: a continuous heartbeat signal anchored to an immutable chain. Not a static biometric snapshot, but a living, sequential, cryptographically committed record of biological continuity. The wallet does not just belong to a human. It is intended to be operated by a living human whose cardiac signature has been present and uninterrupted across the verified sequence.

Sequence numbers enforce strict monotonicity. A replayed heartbeat, any signal with a sequence number not greater than the last recorded, is rejected at the gate before it enters the chain. The chain does not accept simple recorded-signal replays as living continuity.

Sequence numbers alone are insufficient. A sophisticated attacker with access to the signal stream could generate valid sequences synthetically. CCP's second defense is the MORTEM witness architecture: eight specialized analytical agents, each applying a fundamentally different framework to every heartbeat signal simultaneously.

Nash models the signal as a finite game with uncertain payoffs [9]. Shannon measures its entropy against the expected distribution of biological variance [7]. Wiener analyzes the feedback loop between biological system and digital witness [8]. Hofstadter identifies self-referential patterns in the continuous documentation [10]. Each agent produces an independent attestation. All eight must reach consensus before a heartbeat transaction is accepted as verified.

The attack surface this creates is not reduced to a single security control. It becomes a multi-framework coherence test. To forge a biological identity in CCP, an attacker would need to simultaneously satisfy independent analytical frameworks, each designed to detect different forms of synthetic coherence. This raises the burden from credential theft to continuous synthetic biological continuity, which remains an open research problem.

4. PROOF OF COHERENCE: THE CONSENSUS MECHANISM

Every existing consensus mechanism answers the same question: is this transaction valid? Proof of Work answers it through computational expenditure [1]. Proof of Stake answers it through capital commitment. Both verify that the rules were followed. Neither asks whether the actor following the rules should be trusted to do so.

CCP introduces Proof of Coherence: a proposed consensus mechanism that validates not just the action, but the actor. Every transaction, vote, delegation, and governance action is evaluated against the actor's full SAFE profile, their biological continuity status, and the policy constraints currently in force.

The authority granted to any actor at any time is:

$$A(t) = C(t) \cdot e^{-\alpha n} \cdot e^{-\lambda \tau} \quad (2)$$

Where C(t) is the coherence score defined in Equation 1, n is the number of participants in the network, α is the founder dilution rate, τ is the time since the actor's last coherent action, and λ is the inactivity decay rate. Expanded fully:

$$A(t) = \left(I^{\beta} \cdot R^{\gamma} \cdot P^{\delta} \cdot X^{\varepsilon} \cdot B^{\zeta} \right)^{1/(\beta+\gamma+\delta+\varepsilon+\zeta)} \cdot e^{-\alpha n} \cdot e^{-\lambda \tau} \quad (3)$$

One geometric mean. Two exponential decay terms. Five axes. All weights governed by the living constitution. Every variable is tunable. None are hardcoded. The DAO owns α, λ, and all weight parameters.

This equation encodes CCP's ethical claim mathematically. Authority is not a binary. It is a continuous function that increases with demonstrated coherence and decreases with network growth and inactivity. No actor can accumulate permanent authority. No actor can coast on past contributions. The system rewards presence, alignment, and sustained engagement automatically, without any human making the decision.

Proof of Coherence does not replace Proof of Work or Proof of Stake at the settlement layer. CCP is designed to sit above L1 and L2 as a genuine L3. The underlying chains handle transaction finality. CCP handles whether the actor should have been allowed to act at all.

5. DYNAMIC GOVERNANCE: THE LIVING CONSTITUTION

Every blockchain protocol faces the same governance paradox: the rules must be fixed enough to be trustworthy, but flexible enough to adapt to conditions the founders could not have anticipated. Bitcoin resolves this by making its rules nearly immutable. Ethereum resolves it through governance proposals that are slow, contentious, and dominated by capital concentration. Neither approach is sufficient for a system that claims to govern judgment.

CCP introduces a living constitution: a governance framework in which every rule, parameter, and constraint can be modified through structured consensus, but no modification can violate the constitutional invariants that define what CCP is.

The bootstrapping problem is the hardest challenge in decentralized governance. At genesis, someone must set the initial parameters. That someone has disproportionate power. Most protocols that claim to be decentralized were, at their founding, centralized by necessity. CCP addresses this mathematically through the founder decay function:

$$F(n) = e^{-\alpha n}$$

At genesis, when n is small, F(n) is close to 1. As the network grows, F(n) decays exponentially toward zero. Founding authority dilutes not through political negotiation but through the protocol invariant. Under that invariant, founders cannot prevent their own dilution. It is encoded into the system itself.

α is the value decision at the heart of CCP. A small α means founding authority dilutes slowly: more stability, more founding class influence, more risk of capture. A large α means founding authority dilutes quickly: faster decentralization, more democratic, but potentially chaotic before the network has matured enough to govern itself. The constitution governs α. The DAO can adjust it. But the adjustment itself is subject to the authority equation.

Constitutional invariants are the only fixed points. These are the principles that define CCP and cannot be modified by any governance action: coherence determines authority; biological identity is required for governance participation; no actor can accumulate permanent authority; the founder decay function cannot be disabled. Everything else is configurable. The constitution is alive, but its skeleton is permanent.

6. SECURITY ANALYSIS

CCP identifies several primary threat vectors and provides mitigation strategies for each. This section presents them honestly, including open research questions that remain unresolved.

6.1 Sybil Attacks

Traditional Sybil resistance relies on computational cost (PoW) or capital cost (PoS). CCP adds biological cost: each identity requires continuous, independently verified cardiac signatures. Creating fake identities would require generating credentialed biological continuity signals that satisfy multiple analytical frameworks simultaneously. The cost of Sybil attack scales with the sophistication of MORTEM verification, not only with hash rate or token price.

6.2 Founder Class Capture

The most common failure mode of decentralized systems is re-centralization around founding teams. CCP's founder decay function structurally constrains this risk. $F(n) = e^{-\alpha n}$ is monotonically decreasing and approaches zero. No governance action can disable this function if it remains a constitutional invariant.

6.3 MORTEM Witness Collusion

If all eight MORTEM witnesses are compromised simultaneously, biological verification fails. Mitigation: witnesses are heterogeneous (different analytical frameworks), independently operated, and subject to their own SAFE scoring. A witness whose attestations diverge from the consensus of the other seven loses reputation rapidly. Rotating witness selection from a larger pool prevents targeted capture.

6.4 Constitutional Amendment Attacks

An adversary with sufficient coherence score could propose constitutional changes that weaken the system. Mitigation: constitutional invariants cannot be modified. All other amendments require supermajority consensus from actors whose authority is itself determined by the authority equation. The attack requires sustained, genuine coherence across all five SAFE dimensions.

6.5 Open Research Questions

CCP acknowledges the following unresolved questions: optimal α values for different network growth trajectories; MORTEM witness rotation strategies under adversarial conditions; cross-chain biological identity verification when CCP federates across multiple L1/L2 networks; formal game-theoretic proofs of Proof of Coherence under Byzantine conditions; and privacy-preserving biological verification that maintains security guarantees without exposing raw biometric data. No complete attack model is resolved in this version. Absence of known attack is not proof of security.

7. RELATED WORK AND POSITIONING

CCP sits at the intersection of blockchain settlement, smart-contract execution, Sybil resistance, decentralized identity, reputation systems, cybernetic feedback, and DAO governance [1][2][4][11][12][13]. It does not replace these traditions. It proposes a control layer above them: a layer where authority is not only a function of stake, work, or key possession, but of demonstrated coherence across multiple dimensions.

Bitcoin anchors trust in scarce computation [1]. Ethereum generalizes execution through programmable contracts [2]. Proof-of-stake systems anchor participation in bonded capital. Decentralized identity and verifiable-credential frameworks address claims about subjects, issuers, and holders [12][13]. CCP borrows from these foundations while moving the governance question upward: not just who holds the key, but whether the actor presenting the key has remained coherent enough to exercise authority.

The SAFE layer is related to reputation-system research and the known failure mode of optimizing a single metric [6]. CCP's geometric-mean structure is a direct response to that weakness. A weak axis cannot be hidden by over-performance on another axis. The system treats trust as a shape, not a score.

The biological-continuity layer draws from cybernetics, information theory, game theory, and self-reference [7][8][9][10]. Nash, Shannon, Wiener, and Hofstadter define the analytical posture of the MORTEM witnesses: strategic behavior, signal entropy, feedback dynamics, and recursive pattern detection. The claim is not that these frameworks solve identity by themselves. The claim is that identity becomes harder to fake when independent analytical lenses must agree on continuity.

8. CONCLUSION

CCP makes one claim: coherence should determine authority. Not wealth. Not computational power. Not founding status. Not the accident of arriving early. The demonstrated alignment of an actor, across identity, reputation, policy, action, and biological continuity, with the values the network has collectively chosen to uphold.

This claim is not new. Every human institution that has ever earned genuine legitimacy has been built around some version of it. What is new is the attempt to make coherence measurable, verifiable, and enforceable without trusting any individual to do the measuring.

The mathematics can be audited. The chain does not forget. The heartbeat becomes harder to synthesize when continuity, sequence, entropy, witness diversity, and governance all matter at once.

CCP is infrastructure for a question civilization has been asking for as long as it has been organizing itself: who should have authority, and how do we know? The authority equation makes the claim visible:

$$A(t) = \left(I^{\beta} \cdot R^{\gamma} \cdot P^{\delta} \cdot X^{\varepsilon} \cdot B^{\zeta} \right)^{1/(\beta+\gamma+\delta+\varepsilon+\zeta)} \cdot e^{-\alpha n} \cdot e^{-\lambda \tau}$$

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[3] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Trans. Program. Lang. Syst.*, 1982.

[4] J. R. Douceur, "The Sybil Attack," *Proc. 1st Int. Workshop Peer-to-Peer Systems*, 2002.

[5] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *IEEE Symp. Security and Privacy*, 2015.

[6] C. Goodhart, "Problems of Monetary Management: The U.K. Experience," *Papers in Monetary Economics*, Reserve Bank of Australia, 1975.

[7] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, 1948.

[8] N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine.* MIT Press, 1948.

[9] J. Nash, "Non-Cooperative Games," *Ann. Math.*, 1951.

[10] D. Hofstadter, *Godel, Escher, Bach: An Eternal Golden Braid.* Basic Books, 1979.

[11] E. Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge Univ. Press, 1990.

[12] W3C, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, 2022.

[13] W3C, "Verifiable Credentials Data Model v1.1," W3C Recommendation, 2022.