Cardano Foundation

0b19476e40bbbb5e1e8ce153523762e2b6859e7ecacbaf06eae0ee6a447e79b9#0 - Governance Action Voting Rationale

---

1. Governance Action Details

- **Title**: Hard Fork to Protocol Version 10 ("Plomin" Hard Fork)
- **Action ID**: 0b19476e40bbbb5e1e8ce153523762e2b6859e7ecacbaf06eae0ee6a447e79b9#0
- **Type**: Hard Fork Initiation
- **Date Submitted**: 21 December 2024
- **Expiry Date:** 24 January 2025

---

2. Voting Recommendation of Governance Advisory Team

- **Recommendation**: Yes
- **Vote Summary**:
    - **Total Votes**: 7
    - **Votes in Favor**: 6
    - **Votes Against**: 1
    - **Abstentions**: 0
    - **Votes Not to Vote:** 0

3. External Rationale

Summary for Public Communication (summary):

The governance action to hard fork to Protocol Version 10 (“Plomin”) is constitutional. It fulfills all procedural requirements, enables CIP-1694 governance and Plutus primitives, and complies with guardrails. Of note is that a disclosed vulnerability highlights the need for stronger technical safeguards.

Rationale Statement (rationaleStatement):

Understanding the Governance Actions

This governance action, with Action ID *gov_action1pvv5wmjqhwa4u85vu9f4ydmzu2mgt8n7et967ph2urhx53r70xusqnmm52*, aims to upgrade Cardano's mainnet to Protocol Version 10 through the Plomin hard fork. Key changes include:

- Enabling all seven governance actions described in CIP-1694, such as treasury withdrawals, new constitution proposals, and votes of no confidence.
- Activating DRep and SPO voting on applicable governance actions as per CIP-1694.
- Introducing new Plutus primitives, including advanced bitwise operations and RIPEMD-160 cryptographic hashing for improved cross-chain compatibility.
- Restricting staking reward withdrawals to accounts that delegate to a DRep.

Role of the Constitutional Committee

As Article VI, Section 1 of the Interim Constitution outlines, the Constitutional Committee's primary responsibility is to assess the constitutionality of governance actions and vote accordingly. This includes ensuring that all procedural requirements are met to maintain the integrity of the governance process.

Constitutional Compliance

1. **Procedural and Formal Requirements**:

- The proposal adheres to Article III, Section 6, fulfilling requirements for standardization, sufficient rationale, and consistency between off-chain and on-chain documentation.
- The governance action has been verified by Intersect's Hard Fork Working Group and Technical Steering Committee as per the readiness report available at https://cardanoupgrades.docs.intersectmbo.org/plomin-upgrade/chang-upgrade-2-readiness.

2. **Guardrails Compliance:**

- HARDFORK-04: We have used tools such as pooltool.io/networkhealth to monitor the stake pool upgrade status. As of January 22, 2025, ~95% of blocks in the last 24 hours were produced by nodes running protocol version 10-compatible software. This satisfies the guardrail's requirement of 85% adoption by stake pools by stake with updated nodes prior to ratification.
- HARDFORK-01 through HARDFORK-08: The action complies with all guardrails, including versioning, node adoption, and absence of deprecated parameters.
- INTERIM-01: More than 90 days have elapsed since the Chang hard fork, which took place on 1 September 2024, ensuring compliance with interim governance processes.

3. **Impact and Technical Evaluation:**

- Node version 10.1.4 includes safeguards at the mempool level to block specific transaction types that could lead to a denial-of-service (DoS) attack following the hard fork. While this mitigates potential risks at the node level, the vulnerability remains partially addressed, leaving the broader network exposed to malicious blocks.
- The readiness report and widespread 10.1.4 node adoption demonstrate that the ecosystem is technically prepared for the hard fork. As of January 22, 2025, >90% of blocks in the last 24 hours were produced by nodes running node version 10.1.4.

Precedent Discussion (precedentDiscussion)

none

Counterargument Discussion (counterargumentDiscussion)

A key concern involves the disclosed vulnerability and its partial mitigation

- **Issue**: Node version 10.1.4 mitigates DoS risks by introducing mempool-level safeguards to block certain transaction types. However, this fix does not address the broader risk of malicious blocks, which could still exploit the vulnerability post-hard fork. Node users who do not upgrade remain vulnerable.
- **Constitutional Implication**: Article III, Section 6 requires sufficient technical review to ensure governance actions do not endanger the blockchain's security or functionality. The disclosed vulnerability raises questions about the adequacy of the review process and responsible disclosure practices.

Conclusion (conclusion)

The governance action to initiate the Plomin hard fork advancing to Protocol Version 10 is constitutional. It adheres to all procedural requirements and guardrails specified in the Interim Constitution. However, the disclosed vulnerability and its partial mitigation emphasize the need for comprehensive technical reviews and responsible disclosure processes to address network-level risks. The Cardano Foundation, as an ICC member, affirms the constitutionality of this action while urging enhanced practices to safeguard the ecosystem's security and integrity.

Relevant Articles (RelevantArticles)

- Article III, Section 6
- Article VI, Section 1
- Appendix I: Cardano Blockchain Guardrails
    - HARDFORK-01 through HARDFORK-08
    - INTERIM-01
