Draft
02.11.2024

This draft reflects two sets of markup.

1. ***Revisions made as a result of Constitutional Workshop data and Delegate review prior to Nov 01, 2024. These revisions are grayed out.***
2. ***Revisions made based on the consensus reached among the Delegates attending the Costa Rica Workshop. These revisions have gray highlighting.***

CARDANO BLOCKCHAIN ECOSYSTEM CONSTITUTION

PREAMBLE

[This preamble is currently being reviewed and revised by the Cardano Civics Committee]

In the beginning of the Cardano Blockchain ecosystem, three pioneering entities, IOHK, Emurgo, and the Cardano Foundation, came together to foster the emergence of a new blockchain, the Cardano Blockchain, laying the foundation for a decentralized network that would empower individuals, and promote collaboration and innovation. Their pioneering efforts have shaped the path for a blockchain designed to ensure a fair and transparent environment where all participants can contribute to the Cardano Blockchain ecosystem's growth and success.

Over time, the Cardano Blockchain ecosystem has expanded significantly, and now, the Cardano Blockchain ecosystem, comprising of thousands of ada holders, individuals, builders, developers, enterprises, stake pools, users of the Cardano Blockchain and others, operates in a truly decentralized manner, further strengthening the resilience and autonomy of the Cardano Blockchain ecosystem.

As the Cardano Blockchain ecosystem continues to grow, it has become imperative to similarly adapt and evolve its governance model, reflecting the principles of decentralization, community involvement, inclusivity and collaboration that have been the cornerstone of the Cardano Blockchain ecosystem since its start.

Recognizing the need for a more robust and dynamic governance framework, and one that utilizes wherever possible and beneficial blockchain technology in the governance process, the Cardano community, as the members of this decentralized Cardano Blockchain ecosystem, hereby establishes this Cardano Constitution. It shall serve as a guiding set of principles for the operation and governance of our collective efforts, fostering an environment where all participants can contribute to the betterment of the Cardano Blockchain ecosystem as a whole.

Through adopting this Constitution, the Cardano Blockchain ecosystem shall establish a robust governance framework, ensuring that decisions are made in the best interest of the Cardano community. The Cardano community shall uphold principles of transparency, openness, and responsible governance, promoting a culture of trust and collaboration. Together, the Cardano community commits to uphold these principles and to work together towards the continuous improvement, growth, and success of our decentralized blockchain ecosystem known as the Cardano Blockchain.

This Constitution shall serve as the embodiment of these guiding principles for the operation and governance of the decentralized Cardano Blockchain ecosystem, providing a foundation that will adapt and evolve over time to meet the continuing needs of the Cardano community.

All members of the Cardano community are expected to abide by this Constitution, and are entitled to participate in its governance processes, and are encouraged to work collaboratively towards the betterment of the Cardano Blockchain ecosystem as a whole, contributing to its growth, sustainability, and success. The Cardano Blockchain shall be governed on a vote-based decision-making model, fostering inclusivity, a diversity of views, innovation and adaptability. All owners of ada shall have the opportunity to contribute to the governance and direction of the decentralized Cardano Blockchain ecosystem.

In approaching this Constitution, it must be remembered that this is not a constitution for only a blockchain but rather, it is a constitution for a blockchain ecosystem – a much more ambitious endeavor. Accordingly, how governance actions are approved, while extremely important, is not the sole focus of this Constitution. Rather, this Constitution provides the basis and fundamental framework through which all actors in the Cardano Blockchain ecosystem can come together to govern themselves and form radically new approaches to human interaction and collaboration.

By necessity, this Constitution recognizes the role of and empowers the Constitutional Committee, confirms the right of the Cardano community to participate in collective bodies for collaboration, gives effect to on-chain governance, and empowers DReps to act as the voice of ada owners for on-chain voting.

The Constitution also recognizes the necessity of safeguarding access to and the use of funds of the Cardano treasury through the inclusion of the Cardano Guardrails in this Constitution.

ARTICLE I. CARDANO BLOCKCHAIN TENETS AND GUARDRAILS

Section 1

These below Tenets shall guide all actors in the Cardano Blockchain ecosystem including the Constitutional Committee and proposed governance actions shall be evaluated in accordance with these Tenets.

Transactions on the Cardano Blockchain should not be slowed down or censored and should be expediently served for their intended purpose. ~~The Cardano Blockchain should scale taking into consideration throughput, sharding, settlement and dynamic pricing.~~

The cost of transactions on the Cardano Blockchain should be predictable and not unreasonable. ~~The Cardano Blockchain should facilitate an accessible, predictable pricing model.~~

Anyone desiring to develop and deploy applications on the Cardano Blockchain should not unreasonably be prevented from developing and deploying such applications as intended. ~~The Cardano community should promote features to assist in developing and deploying applications such as digital subscriber lines, formal verification support, asynchronous and scalable location services, oracles and access to partnerchains.~~

Contributions by the Cardano community on the Cardano Blockchain should be recognized, recorded and assessed fairly by the Cardano community through reward sharing with SPOs and DReps, appropriate tokenomics and multi-resource consensus approaches.

The Cardano Blockchain shall not lock in an ada owner's value without an owner's consent. The Cardano Blockchain should promote interoperability and access to partnerchains.
The Cardano Blockchain shall preserve in a safe manner any value and information an owner of ada seeks to store on the Cardano Blockchain. To assure safe protection of value and information, the Cardano Blockchain should focus on integrity, post-quantum security, decentralization and decentralized storage, access to stablecoins and robust key management approaches.

The Cardano Blockchain should promote interoperability and access to partnerchains.

The Cardano Blockchain shall preserve in a safe manner any value and information an ada owner seeks to store on the Cardano Blockchain.

The Cardano Blockchain shall not unnecessarily spend resources. The Cardano Blockchain shall promote efficient design, memory and storage.

All users of the Cardano Blockchain shall be treated equally taking into account the collective desires of the Cardano Blockchain community consistent with the long-term sustainability and viability of the Cardano Blockchain. Long-term sustainability and viability shall be evaluated by a number of considerations including fairness, neutrality, sustainability, robust governance, promotion of decentralized identity, use of multi-resource consensus and democratic participation by all members of the Cardano community.

Financial stability shall be maintained. and the total supply of ada shall not exceed 45,000,000,000 (45,000,000,000,000,000) Lovelace

Workshop Questions

• Do you believe these tenets appropriately reflect the ethos of the Cardano Blockchain? • Should there be an additional tenet addressing financial sustainability? If yes, what should it contain? Should it include an absolute cap on the circulating supply of ada?

[Future Workstream: Address a supply cap]

Section 2

The Cardano Blockchain shall operate in accordance with the Cardano Blockchain Guardrails as set forth in the Guardrails Appendix to this Constitution. The Cardano community may from time to time digitally codify certain Cardano Blockchain Guardrails such that such Cardano Blockchain Guardrails are directly programmed and implemented on the Cardano Blockchain using on-chain scripts or built-in ledger rules.

In the event there are inconsistencies between a Cardano Blockchain Guardrail as set forth in the Guardrails Appendix and any such Cardano Blockchain Guardrail that has been programmed and implemented on the Cardano Blockchain, the version of such Cardano Blockchain Guardrail that has been deployed directly on the Cardano Blockchain shall prevail and the Constitutional Committee shall seek to reconcile such inconsistencies through the encouragement of an appropriate on-chain governance action.

ARTICLE II. THE CARDANO BLOCKCHAIN COMMUNITY

Section 1

No formal membership shall be required to use, participate in and benefit from the Cardano Blockchain. Instead, all owners of ada, all developers of, all those building on, and all those otherwise supporting, maintaining or using the Cardano Blockchain are beneficiaries of the Cardano Blockchain ecosystem and, as such, are collectively members of the Cardano community. All Cardano community members are accordingly beneficiaries of this Constitution, entitled to its rights, privileges and protections and, as such, are expected to support and uphold this Constitution.

Section 2

Members of the Cardano community who own ada~~*[, as well as their appointed designees,]*~~ are entitled to access and participate in the on-chain decision-making processes of the Cardano Blockchain ecosystem, including voting and taking part in on-chain governance regarding the Cardano Blockchain.

~~*Workshop Questions*~~

~~*• Should on-chain governance participation be limited to only owners of ada or should ada owners be allowed to appoint designees who are then entitled to participate in on chain governance? [Note that this is not a reference to delegation to DReps.]*~~

Section 3

Members of the Cardano community have a responsibility to maintain the integrity of the Cardano Blockchain ecosystem by following this Constitution, operating the Cardano Blockchain network, participating in Cardano Blockchain governance activities, and resolving disputes in a fair and transparent manner.

Section 4

The Cardano community is entitled and encouraged through the provisions of this Constitution to collaborate in developing, maintaining and building applications for the Cardano community, and to form temporary and permanent organizations and entities as the Cardano community deems desirable or appropriate in support of the Cardano Blockchain ecosystem.

ARTICLE III. PARTICIPATORY GOVERNANCE

Draft
02.11.2024

Section 1

The Cardano Blockchain ecosystem shall be governed by a decentralized, on-chain governance model, utilizing, to the extent possible and beneficial, smart contracts and other blockchain based tools to facilitate decision-making and ensure transparency. On-chain voting for governance actions shall follow the process outlined in the Cardano Blockchain Guardrails.

Section 2

Three independent governance bodies shall participate in voting for on-chain governance actions to provide checks and balances for the Cardano Blockchain consisting of Delegated Representatives (DRep), Stake Pool Operators (SPO) and the Constitutional Committee (CC).

Section 3

On-chain governance decisions shall be made through a collective decision-making process, with specific consensus threshold requirements as required by the Cardano Blockchain Guardrails. All on-chain governance actions shall be voted upon in accordance with the Cardano Blockchain Guardrails.

Section 4

All owners of ada~~*[, as well as their appointed designees,]*~~ shall have the right to vote in on-chain governance action decision-making processes, subject to any restrictions or requirements provided for in this Constitution and the Cardano Blockchain Guardrails.

~~*Workshop Questions*~~

- ~~*Voting rights are in proportion to the ada owned. However, should the Constitution specify a specific voting model?*~~
- ~~*Should the Constitution enshrine one ada one vote?*~~
- ~~*How do we address participation by institutions? Should holders of ada who are not owners, such as exchanges, be allowed to vote?*~~

~~All owners of ada*[, as well as their appointed designees,]* shall have the right to propose changes to the governance structure of the Cardano Blockchain ecosystem in accordance with the Cardano Blockchain Guardrails.~~ All owners of ada shall have the right to propose changes to the governance structure of the Cardano Blockchain ecosystem in accordance with the Cardano Blockchain Guardrails. Owners of ada who use third-party custodians or other designees to hold their ada, may authorize, or may withhold authorization for, such third-parties to vote on their behalf.

[Future Workstream: Explanatory material for authorized designees that helps to clarify what it means for ada owners and custodians]

Section 5

A special form of governance action exists to allow community sentiment to be gauged without committing to any on-chain change of the Cardano Blockchain. "Info" actions have no on-chain effect other than to record the outcome of such a vote on the Cardano Blockchain.

Section 6

Any proposed on-chain governance action shall require a standardized and legible format including a URL and hash linked to documented off-chain content. Sufficient rationale shall be provided to justify the requested change to the Cardano Blockchain. The rationale shall include, at a minimum, a title, abstract, reason for the proposal, and relevant supporting materials.

Any governance action proposal reaching the on-chain governance stage shall be identical in content as to the final off-chain version of such governance action proposal.

“Hard Fork Initiation” and “Protocol Parameter Change” governance actions should undergo sufficient technical review and scrutiny as mandated by the Cardano Blockchain Guardrails to ensure that the governance action does not endanger the security, functionality, ~~or~~ performance or long-term sustainability of the Cardano Blockchain. On-chain governance actions should address their expected impact on the Cardano Blockchain ecosystem.

All owners of ada shall have the right to ensure that the process for participating in, submitting and voting on on-chain governance actions is open and transparent and is protected from undue influence and manipulation.

Section 7

The Cardano community is expected to support the creation, maintenance and ongoing administration of off-chain governance processes as may be necessary to give effect to this Constitution and to ensure that there is awareness of and an opportunity to debate and shape all future governance actions for the Cardano Blockchain.

Section 8

The Cardano community is expected to propose, not less than on an annual basis, a budget for the ongoing maintenance and future development of the Cardano Blockchain. All owners of ada~~*[, as well as their appointed designees,]*~~ are expected to periodically approve the Cardano Blockchain budget through an on-chain “Info action.”~~governance action.~~ No withdrawals from the Cardano Blockchain treasury shall be permitted unless a budget for the Cardano Blockchain, that has not been determined by the Constitutional Committee to be unconstitutional, is then in effect as required by the Cardano Blockchain Guardrails. Cardano Blockchain budgets shall specify a process for overseeing use of funds from Cardano Blockchain treasury withdrawals including designating one or more administrators who shall be responsible for such oversight.

~~*[*~~Any governance action requesting ada from the Cardano Blockchain treasury ~~*in excess of [1,000,000] ada*~~ shall require an allocation of ada as a part of such funding request to cover the

cost of periodic independent audits and the implementation of oversight metrics as to the use of such ada.~~] [~~Contractual obligations governing the use of ada received from the Cardano Blockchain treasury pursuant to a Cardano budget ~~*in excess of [1,000,000] shall include dispute resolution provisions.]*~~ shall include dispute resolution provisions.

[Future Workstream: Continue to mature the Cardano Budget process and define how to implement the audit, metrics and dispute resolution requirements; DReps to approve a net change limit for the Cardano treasury as part of the budget process.]

~~*Workshop Questions*~~

- ~~*Should the Constitution require that governance actions above a specified amount include allocations of ada to cover periodic audits and implementation of oversight metrics? If yes, how should they be enforced?*~~
- ~~*Should the Constitution require that contractual provisions governing the use of ada received from the treasury above a specified amount include dispute resolution provisions? If yes, how should they be enforced?*~~
- ~~*Should the Constitution require that the budget include a contingency fund? If so, how would it work? What could it be used for? Who would administer it?*~~
- ~~*Should the Constitution require that the budget include an indemnity fund to cover potential claims against governance participants such as DReps and Constitutional Committee members? If so, how would it work? What could it be used for? Who would administer it?*~~
- ~~*Should the budgetary process be spelled out in greater detail in the Constitution? Should the Constitution identify how the budget will be administered? Should it identify who will administer the budget?*~~
- ~~*Should the Constitution specify a cap on the annual budget?*~~

ARTICLE IV. DELEGATED REPRESENTATIVES

Section 1

In order to participate in governance actions, owners of ada may register as DReps and directly vote on such governance actions or may delegate their voting rights to other registered DReps who shall vote on their behalf.

Section 2

Any owner of ada shall have the option to register as a DRep. Any owner of ada~~*[, as well as their appointed designees,]*~~ shall be allowed to delegate their voting stake to one or more registered DReps, including themselves. DReps may be individuals or coordinated groups.

Owners of ada who use third-party custodians or other designees to hold their ada, may authorize, or may withhold authorization for, such third-parties to delegate voting rights to registered DReps on their behalf. DReps are entitled to cast votes directly for on-chain governance actions and represent those ada holders delegating their voting rights to them.

This voting system shall enshrine a liquid democracy model where owners of ada can seamlessly select among DReps, register as a DRep, and change their delegation at any time.

Section 3

~~/~~DReps are expected to adopt codes of conduct from time to time governing their activities as DReps and make such codes of conduct publicly available.~~/~~ DReps codes of conduct should include disclosure requirements addressing situations where DReps are also SPOs and are participating in on-chain governance actions in both capacities. [[the previous proposed sentence was redacted in the Costa Rica workshop and covered solely in Article V, Section 4.]]

[Future Workstream: Individual vs unified, or basic requirements of a code of conduct can be determined by the community over time, e.g., using CIPs or Info actions; Develop community standards for DRep codes of conduct]

~~*Workshop Questions*~~

~~• Should the Constitution include any guidelines as to the requirements that must be included by DReps in their respective codes of conduct?~~

~~• Should there be one code of conduct for all DReps or should each DRep be allowed to adopt its own code of conduct? Should DRep codes of conduct be on-chain? • Should the Constitutional Committee determine whether such codes of conduct are consistent with the Constitution?~~

~~• Should the Constitution include term limits for DReps?~~

Section 4

The Cardano community is expected to support the creation, maintenance and ongoing administration of tools to enable owners of ada to explore and evaluate DRep candidates and select DReps on such criteria as they deem relevant.

Section 5

~~/~~DReps may be compensated for their efforts ~~to foster the creation of a professional governance cohort for the Cardano Blockchain ecosystem~~. DReps shall ensure that any compensation received in connection with their activities as a DRep is disclosed. DReps may not otherwise purchase voting rights.~~/~~

[Future Workstream: Mechanism for DRep compensation]

Workshop Questions

• Should the Constitution mandate compensation for DReps? If so, should the Constitution specify how compensation is determined or include a cap on compensation? • Should the Constitution require that budgets approved for the Cardano Blockchain include an allocation from the Cardano Blockchain treasury sufficient to compensate DReps in such amounts as may be approved from time to time by ada owners.

ARTICLE V. STAKE POOL OPERATORS

Section 1

SPOs shall have a specific role in approving critical on-chain governance actions which require additional oversight and independence, voting separately and independently from DReps as set forth in the Cardano Blockchain Guardrails. SPOs shall participate in hard fork initiation processes as the operators of the nodes that participate in Cardano Blockchain's consensus mechanism.

Section 2

SPOs may act as a check on the power of the Constitutional Committee under exceptional circumstances by separately voting on "Motion of no-confidence" and "Update committee/threshold" governance actions, and on "Parameter Update" governance actions that affect security-critical parameters."

Section 3

[Owners of ada who are both DReps and SPOs shall either refrain from voting in on-chain governance actions in both capacities or shall publicly disclose that they SPOs are encouraged to adopt codes of conduct from time to time governing their activities as SPOs and make such codes of conduct publicly available. SPO codes of conduct should include disclosure requirements addressing situations where SPOs are also DReps and are participating in on-chain governance actions in both capacities. *such capacities prior to exercising any on-chain governance rights.]* [[the previous proposed sentence was redacted in the Costa Rica workshop and covered solely in Article V, Section 4.]]

[Future Workstream: Requirement for SPOs codes of conduct, if any; Create educational materials to clarify how ada owners maintain power separation and encourage more data sources that allow ada owners to make informed decisions; address "sticky" SPO and DRep delegation possibly through a new CIP]

Workshop Questions

• Should the Constitution include a requirement that ada owners who are both DReps and SPOs either refrain from voting in both capacities or disclose such dual roles? • Should the Constitution include other conflicts of interest provisions included? • Should the Constitution require that SPOs be expected to implement codes of conduct? If yes, should they be on-chain? Should the Constitutional Committee determine whether such codes of conduct are consistent with the Constitution?]

ARTICLE VI. CONSTITUTIONAL COMMITTEE

Section 1
A Constitutional Committee shall be established as the branch of Cardano's on-chain governance process that ensures governance actions are consistent with this Constitution. The Constitutional Committee shall comprise a set of owners of ada*[, including their appointed designees,]* that is collectively responsible for ensuring that on-chain governance actions, excluding Info actions, [[the previous proposed edit was redacted in the Costa Rica workshop and addressed instead in Section 4 below]] prior to enactment on chain, are constitutional. The Constitutional Committee shall be limited to voting on the constitutionality of governance actions, excluding Info actions. [[the previous proposed edit was redacted in the Costa Rica workshop and addressed instead in Section 4 below]] Constitutional Committee members are expected to have appropriate expertise to carry out their required responsibilities, considering their past contributions and involvement in the Cardano Blockchain ecosystem.

Section 2

The Constitutional Committee shall be composed of *[*such number of members as shall be determined from time to time by owners of ada*]*, as consistent with the Cardano Blockchain Guardrails, and as shall be sufficient to assure the ongoing integrity of the Cardano Blockchain.

Workshop Questions

• Should the Constitution specify how the number of members of the CC are determined? [Note that the Guardrails specify both a minimum and maximum number of members.]

Members of the Constitutional Committee shall serve such terms *[*lengths as shall be determined from time to time by owners of ada*]* as consistent with the Cardano Blockchain Guardrails, provided that terms shall not be less than one year minimum and maximum term lengths as set forth in the Cardano Blockchain Guardrails. To assure continuity in the operation of the Constitutional Committee, the terms for Constitutional Committee members shall be staggered.

[Future Workstream: A process for determining the size and term length for the CC]

Workshop Questions

~~• *Should the Constitution specify how term limits for CC members are determined? [Note that the Guardrails specify both a minimum and maximum term limit.]*~~

Section 3

The Cardano community shall establish a process from time to time for election of members of the Constitutional Committee consistent with the requirements of the Cardano Blockchain Guardrails.

[Future Workstream: Identifying the election process; community education]

~~*Workshop Questions*~~

~~• *Should the Constitution include an explicit process for the election of members of the CC?*~~

Section 4

No governance action, other than a "Motion of no-confidence," ~~or~~ "Update constitutional committee/threshold" or "Info action" may be implemented on-chain unless the Constitutional Committee shall have first determined and affirmed through an on-chain action that such proposal does not violate this Constitution. In the case of "Info actions," which are never enacted on chain, the Constitutional Committee shall refrain from voting or may vote abstain on the "Info actions," except that in the case of "Info actions" that propose a Cardano Blockchain budget, the Constitutional Committee shall determine whether such a proposed Cardano Blockchain budget, if implemented, would violate this Constitution.

The Constitutional Committee shall be considered to be in one of the following two states at all times: a state of confidence or a state of no-confidence. In a state of no-confidence, members of the then standing Constitutional Committee must be reinstated or replaced using the "Update committee/threshold" governance action before any other on-chain governance action may go forward.

Section 5

Constitutional Committee processes shall be transparent. The Constitutional Committee shall publish each decision. When voting ~~[~~*no*~~]~~ on a proposal, ~~[~~the Constitutional Committee~~] [~~ collectively, or each member of the Constitutional committee casting a no vote~~]~~ separately shall set forth the basis for its decision with reference to specific Articles of this Constitution or provisions of the Guardrails Appendix that are in conflict with a given proposal.

The Constitutional Committee shall operate pursuant to a code of conduct published by the Constitutional Committee from time to time and shall adopt such policies and procedures as the Constitutional Committee shall deem necessary in carrying out its duties.

[Future Workstream: Should the Constitution require that the Constitutional Committee code of conduct be on chain and should the community have any role in approving the

Constitutional Committee code of conduct?]

Workshop Questions

• Should the Constitution require that the Constitutional Committee code of conduct be on chain?

• Should the community have any role in approving the Constitutional Committee code of conduct? If so, how would this work?

Section 6

The Cardano community is expected to support the creation, maintenance and ongoing administration of tools as may be necessary and appropriate for the Constitutional Committee to perform its required functions.

Section 7

*[*Constitutional Committee members may be compensated for their efforts as members of the Constitutional Committee. Constitutional Committee members shall ensure that any compensation received in connection with their activities as a member is disclosed.*]* *[*Budgets approved for the Cardano Blockchain shall include allocations from the Cardano Blockchain treasury sufficient to *[*compensate Constitutional Committee members in such amounts as may be approved from time to time by ada owners*]* and to provide for periodic administrative costs of the Constitutional Committee in such amounts as requested from time to time by the Constitutional Committee and as may be approved by ada owners.*]*

[Future Workstream: Process as to how compensation is determined as well as a potential cap on compensation and process for overseeing administrative expenditures by the CC including potential audit oversight; Require that the budget process follow best practices, which would include a contingency provision.]

Workshop Questions

• Should the Constitution mandate compensation for CC members? If so, should the Constitution specify how compensation is determined or include a cap on compensation? • Should the Constitution require that budgets approved for the Cardano Blockchain include an allocation from the Cardano Blockchain treasury sufficient to compensate CC members in such amounts as may be approved from time to time by ada owners. • Should the Constitution require that the budget include an allocation for the administrative costs of the CC? If so, how should the amount be determined? If so, should the Constitution specify who would administer such a budget and whether expenditures by the CC should be public or subject to audit oversight?

ARTICLE VII. AMENDMENTS

Draft
02.11.2024

Section 1

Except as otherwise so provided in the Cardano Blockchain Guardrails Appendix, amendments to this Constitution, including to the Cardano Blockchain Guardrails Appendix, shall be approved by a collective decision-making process, requiring an on-chain governance action by owners of ada~~*[, including their appointed designees,]*~~ satisfying a threshold of not less than 67% of the then active voting stake.

Section 2

If the Cardano Blockchain Guardrails Appendix sets forth an amendment threshold for a Cardano Blockchain Guardrail that~~-is~~ are different than the amendment threshold contained in Section 1 of this Article VII, then the threshold set forth in the Cardano Blockchain Guardrails Appendix for such Cardano Blockchain Guardrail shall apply.

[Future Worktsream: Continued discussion of amendment process including potential separate amendment thresholds for Guardrails]

~~*Workshop Questions*~~

~~• *Should the Constitution include a provision preventing Article VII itself from being amended or allowing any governance action that would have the effect of changing these amendment requirements?*~~

~~• *Should the Constitution include a category of technical guardrail modifications that could be overseen and approved by the Constitutional Committee? Is this even possible? If yes, should such a category be narrowly defined to only address high security risks or emergency issues?*~~

Draft
02.11.2024

APPENDIX I: CARDANO BLOCKCHAIN GUARDRAILS

1. INTRODUCTION

To implement Cardano Blockchain on-chain governance ~~pursuant to CIP-1694~~, it is necessary to establish sensible guardrails that will enable the Cardano Blockchain to continue to operate in a secure and sustainable way.

This Appendix sets forth guardrails that must be applied to Cardano Blockchain on-chain governance actions, including changes to the protocol parameters and limits on treasury withdrawals. These guardrails cover both essential, intrinsic limits on settings, and recommendations that are based on experience, measurement and governance objectives.

These guardrails are designed to avoid unexpected problems with the operation of the Cardano Blockchain. They are intended to guide the choice of sensible parameter settings and avoid potential problems with security, performance, ~~or~~ functionality or long-term sustainability. As described below, some of these guardrails are automatable and will be enforced via an on-chain script or built-in ledger rules.

These guardrails apply to the Cardano Blockchain Layer 1 mainnet environment. They are not intended to apply to test environments or to other blockchains that use the Cardano Blockchain software.

Not all parameters for the Cardano Blockchain can be considered independently. Some parameters interact with other settings in an intrinsic way. Where known, these interactions are addressed in this Appendix.

While the guardrails in this Appendix presently reflect the current state of technical insight, this Appendix should be treated as a living document. Implementation improvements, new simulations or performance evaluation results for the Cardano Blockchain may allow some of the restrictions contained in these guardrails to be relaxed (or, in some circumstances, require them to be tightened) in due course.

Additional guardrails may also be needed where, for example, new protocol parameters are introduced.

The guardrails set forth in this Appendix may be amended from time to time pursuant to an on chain governance action that satisfies the applicable voting threshold as set forth in this Appendix. Any such amendment to any guardrails shall require and be deemed to be an amendment to the Constitution itself.

~~*Workshop Questions*~~

~~*• Should any of the below Guardrails include an amendment threshold different from the threshold included in Article VII?*~~

Terminology and Guidance

Should/Should not. Where this Appendix says that a value "should not" be set below or

above some value, this means that the guardrail is a recommendation or guideline, and the specific value could be open to discussion or alteration by a suitably expert group recognized by the Cardano community in light of experience with the Cardano Blockchain governance system or the operation of the Cardano Blockchain.

Must/Must not. Where this Appendix says that a value "must not" be set below or above some value, this means that the guardrail is a requirement that will be enforced by Cardano Blockchain ledger rules, types or other built-in mechanisms where possible, and that if not followed could cause a protocol failure, security breach or other undesirable outcome.

Benchmarking. Benchmarking refers to careful system level performance evaluation that is designed to show a-priori that, for example, 95% of blocks will be diffused across a global network of Cardano Blockchain nodes within the required 5s time interval in all cases. This may require construction of specific test workflows and execution on a large test network of Cardano nodes, simulating a global Cardano Blockchain network.

Performance analysis. Performance analysis refers to projecting theoretical performance, empirical benchmarking or simulation results to predict actual system behavior. For example, performance results obtained from tests in a controlled test environment (such as a collection of data centers with known networking properties) may be extrapolated to inform likely performance behavior in a real Cardano Blockchain network environment.

Simulation. Simulation refers to synthetic execution that is designed to inform performance/functionality decisions in a repeatable way. For example, the IOSim Cardano Blockchain module allows the operation of the networking stack to be simulated in a controlled and repeatable way, allowing issues to be detected before code deployment.

Performance Monitoring. Performance monitoring involves measuring the actual behavior of the Cardano Blockchain network, for example, by using timing probes to evaluate round-trip times, or test blocks to assess overall network health. It complements benchmarking and performance analysis by providing information about actual system behavior that cannot be obtained using simulated workloads or theoretical analysis.

Reverting Changes. Where performance monitoring shows that actual network behavior following a change is inconsistent with the performance requirements for the Cardano Blockchain, then the change must be reverted to its previous state if that is possible. For example, if the block size is increased from 100KB to 120KB and 95% of blocks are no longer diffused within 5s, then a change must be made to revert the block size to 100KB. If this is not possible, then one or more alternative changes must be made that will ensure that the performance requirements are met.

Severity Levels. Issues that affect the Cardano Blockchain network are classified by severity level, where:

- Severity 1 is a critical incident or issue with very high impact to the security, performance, ~~or~~ functionality or long-term sustainability of the Cardano Blockchain network
- Severity 2 is a major incident or issue with significant impact to the security,

performance, ~~or~~ functionality or long-term sustainability of the Cardano Blockchain network
- Severity 3 is a minor incident or issue with low impact to the security, performance, ~~or~~ functionality or long-term sustainability of the Cardano Blockchain network

Future Performance Requirements. Planned development such as new mechanisms for out of memory storage may impact block diffusion or other times. When changing parameters, it is necessary to consider these future performance requirements as well as the current operation of the Cardano Blockchain. Until development is complete, the requirements will be conservative; they may then be relaxed to account for actual timing behavior.

Automated Checking ("Guardrails Script")

A script hash is associated with the constitution hash when a **New Constitution or Guardrails Script** governance action is enacted. It acts as an additional safeguard to the ledger rules and types, filtering non-compliant governance actions.

The guardrails script only affects two types of governance actions:

- **Parameter Update** actions, and
- **Treasury Withdrawal** actions.

The script is executed when either of these types of governance action is submitted on-chain. This avoids scenarios where, for example, an erroneous script could prevent the chain from ever enacting a Hard Fork action, resulting in deadlock. There are three different situations that apply to script usage.

Symbol and Explanation

- (y) The script can be used to enforce the guardrail.
- (x) The script cannot be used to enforce the guardrail.
- (~ - reason) The script cannot be used to enforce the guardrail for the reason given, but future ledger changes could enable this.

Guardrails may overlap: in this case, the most restrictive set of guardrails will apply.

Where a parameter is not explicitly listed in this document, then the script **must not** permit any changes to the parameter.

Conversely, where a parameter is explicitly listed in this document but no checkable guardrails are specified, the script **must not** impose any constraints on changes to the parameter.

2. GUARDRAILS AND GUIDELINES ON PROTOCOL PARAMETER UPDATE ACTIONS

Below are guardrails and guidelines for changing updatable protocol parameter settings via the protocol parameter update governance action such that the Cardano Blockchain is never in an unrecoverable state as a result of such changes.

Note that there are at least five different sources of parameter names, and these are not always consistent:

1. The name used in the Genesis file
2. The name used in protocol parameter update governance actions
3. The name used internally in ledger rules
4. The name used in the formal ledger specification
5. The name used in research papers

Where these parameter names differ, this Appendix uses the second

convention.

Guardrails

PARAM-01 (y) Any protocol parameter that is not explicitly named in this document **must not** be changed by a Parameter update governance action

PARAM-02 (y) Where a protocol parameter is explicitly listed in this document but no checkable guardrails are specified, the guardrails script **must not** impose any constraints on changes to the parameter. Checkable guardrails are shown by a (y)

2.1. Critical Protocol Parameters

The below protocol parameters are critical from a security point of

view. *Parameters that are Critical to the Operation of the Blockchain*

- *maximum block body size* (*maxBlockBodySize*)
- *maximum transaction size* (*maxTxSize*)
- *maximum block header size* (*maxBlockHeaderSize*)
- *maximum size of a serialized asset value* (*maxValueSize*)
- *maximum script execution/memory units in a single block* (*maxBlockExecutionUnits[steps/memory]*)
- *minimum fee coefficient* (*txFeePerByte*)
- *minimum fee constant* (*txFeeFixed*)
- *minimum fee per byte for reference scripts* (*minFeeRefScriptCoinsPerByte*) - *minimum Lovelace deposit per byte of serialized UTxO* (*utxoCostPerByte*) - *governance action deposit* (*govDeposit*)

Guardrails

PARAM-03 (y) Critical protocol parameters require an SPO vote in addition to a DRep vote: SPOs **must** say "yes" with a collective support of more than 50% of all active block production stake. This is enforced by the guardrails on the stake pool voting threshold.

PARAM-04 (x) At least 3 months **should** normally pass between the publication of an off chain proposal to change a critical protocol parameter and the submission of the corresponding on-chain governance action. This guardrail may be relaxed in the event of a Severity 1 or Severity 2 network issue following careful technical discussion and evaluation.

Parameters that are Critical to the Governance System

- *delegation key Lovelace deposit* (*stakeAddressDeposit*)
- *pool registration Lovelace deposit* (*stakePoolDeposit*)
- *minimum fixed rewards cut for pools* (*minPoolCost*)
- *DRep deposit amount* (*dRepDeposit*)
- *minimal Constitutional Committee size* (*committeeMinSize*)
- *maximum term length (in epochs) for the Constitutional Committee members* (*committeeMaxTerm~~Limit~~Length*)

Guardrails

PARAM-05 (y) DReps **must** vote "yes" with a collective support of more than 50% of all active voting stake. This is enforced by the guardrails on the DRep voting thresholds.

PARAM-06 (x) At least 3 months **should** normally pass between the publication of an off chain proposal to change a parameter that is critical to the governance system and the submission of the corresponding on-chain governance action. This guardrail may be relaxed in the event of a Severity 1 or Severity 2 network issue following careful technical discussion and evaluation.

2.2. Economic Parameters

The overall goals when managing economic parameters are to:

1. Enable long-term economic sustainability for the Cardano Blockchain ecosystem;
2. Ensure that stake pools are adequately rewarded for maintaining the Cardano Blockchain;
3. Ensure that ada holders are adequately rewarded for using stake in constructive ways, including when delegating ada for block production; and
4. Balance economic incentives for different Cardano Blockchain ecosystem stakeholders, including but not limited to Stake Pool Operators, ada holders, DeFi users, infrastructure users, developers (e.g. DApps) and financial intermediaries (e.g. exchanges)

Triggers for Change

1. Significant changes in the fiat value of ada resulting in potential problems with security, performance, ~~or~~ functionality or long-term sustainability
2. Changes in transaction volumes or types
3. Community requests or suggestions
4. Emergency situations that require changes to economic parameters

Counter-indicators

Changes to the economic parameters should not be made in isolation. They need to account for:

- External economic factors
- Network security concerns

Core Metrics

- Fiat value of ada resulting in potential problems with security, performance, ~~or~~ functionality or long-term sustainability
- Transaction volumes and types
- Number and health of stake pools
- External economic factors

Changes to Specific Economic Parameters

Transaction fee per byte (txFeePerByte) and fixed transaction fee

(txFeeFixed) Defines the cost for basic transactions in Lovelace:

fee(tx) = txFeeFixed + txFeePerByte x nBytes(tx)

Guardrails

TFPB-01 (y) *txFeePerByte* **must not** be lower than 30 (0.000030 ada)
This protects against low-cost denial of service attacks

TFPB-02 (y) *txFeePerByte* **must not** exceed 1,000 (0.001 ada)
This ensures that transactions can be paid for

TFPB-03 (y) *txFeePerByte* **must not** be negative

TFF-01 (y) *txFeeFixed* **must not** be lower than 100,000 (0.1 ada)
This protects against low-cost denial of service attacks

TFF-02 (y) *txFeeFixed* **must not** exceed 10,000,000 (10 ada)
This ensures that transactions can be paid for
TFF-03 (y) *txFeeFixed* **must not** be negative

TFGEN-01 (x - "should") To maintain a consistent level of protection against denial-of-service attacks, *txFeeFixed* and *txFeeFixed* **should** be adjusted whenever Plutus Execution prices are adjusted (executionUnitPrices[steps/memory])

TFGEN-02 (x - unquantifiable) Any changes to *txFeeFixed* or *txFeeFixed* **must** consider the implications of reducing the cost of a denial-of-service attack or increasing the maximum transaction fee so that it becomes impossible to construct a transaction.

UTxO cost per byte (utxoCostPerByte)

Defines the ~~cost for storage in UTxOs~~ deposit (in Lovelace) that is charged for each byte of storage that is held in a UTxO. This deposit is returned when the UTxO is no longer active.

- Sets a minimum threshold on ada that is held within a single UTxO
(~1 ada minimum, could be >= 50 ada in the worst case)
- Provides protection against low-cost denial of service attack on UTxO storage. This attack has been executed on other chains - it is not theoretical.
DoS protection decreases in line with the free node memory (proportional to UTxO growth)
    - Helps reduce long term storage costs for node users by providing an incentive to return UTxOs when no longer needed, or to merge UTxOs.
    - ~~Provides an incentive to return UTxOs when no longer needed.~~
~~Should significantly exceed minimum tx cost (~ 0.15 ada)~~

Guardrails

UCPB-01 (y) *utxoCostPerByte* **must not** be lower than 3,000 (0.003

ada) UCPB-02 (y) *utxoCostPerByte* **must not** exceed 6,500 (0.0065

ada) UCPB-03 (y) *utxoCostPerByte* **must not** be zero

UCPB-04 (y) *utxoCostPerByte* **must not** be negative

UCPB-05 (x - "should") Changes **should** account for

i) The acceptable cost of attack
ii) The acceptable time for an attack ~~(at least one epoch is assumed)~~
iii) The acceptable memory configuration for full node users ~~(assumed to be 16GB for wallets or 24GB for stake pools)~~
iv) The sizes of UTxOs ~~(~200B per UTxO minimum, up to about 10KB)~~ and
v) The current total node memory usage

Stake address deposit (stakeAddressDeposit)

Ensures that stake addresses are retired when no longer needed
- Helps reduce long term storage costs
- Helps limit CPU and memory costs in the ledger

The rationale for the deposit is to incentivize that scarce memory resources are returned when they are no longer required. Reducing the number of active stake addresses also reduces processing and memory costs at the epoch boundary when calculating stake snapshots.

Guardrails

SAD-01 (y) *stakeAddressDeposit* **must not** be lower than 1,000,000 (1 ada)

SAD-02 (y) *stakeAddressDeposit* **must not** exceed 5,000,000 (5 ada)

SAD-03 (y) *stakeAddressDeposit* **must not** be negative

Stake pool deposit (stakePoolDeposit)

Ensures that stake pools are retired by the stake pool operator when no longer needed by them

- Helps reduce long term storage costs

The rationale for the deposit is to incentivize that scarce memory resources are returned when they are no longer required. Rewards and stake snapshot calculations are also impacted by the number of active stake pools.

Guardrails

SPD-01 (y) *stakePoolDeposit* **must not** be lower than 250,000,000 (250

ada) SPD-02 (y) *stakePoolDeposit* **must not** exceed 500,000,000 (500 ada)

SPD-03 (y) *stakePoolDeposit* **must not** be negative

Minimum Pool Cost (minPoolCost)

Part of the rewards mechanism

- The minimum pool cost is transferred to the pool rewards address before any delegator rewards are paid

Guardrails

MPC-01 (y) *minPoolCost* **must not** be negative

MPC-02 (y) *minPoolCost* **must not** exceed 500,000,000 (500 ada)

MPC-03 (x - "should") *minPoolCost* **should** be set in line with the economic cost for operating a pool

Treasury Cut (treasuryCut)

Part of the rewards mechanism

- The treasury cut portion of the monetary expansion is transferred to the treasury before any pool rewards are paid

- Can be set in the range 0.0-1.0 (0%-100%)

Guardrails

TC-01 (y) *treasuryCut* **must not** be lower than 0.1 (10%)

TC-02 (y) *treasuryCut* **must not** exceed 0.3 (30%)

TC-03 (y) *treasuryCut* **must not** be negative

TC-04 (y) *treasuryCut* **must not** exceed 1.0 (100%)

TC-05 (~ - no access to change history) *treasuryCut* **must not** be changed more than once in any 36 epoch period (approximately 6 months)

Monetary Expansion Rate (monetaryExpansion)

Part of the rewards mechanism

- The monetary expansion controls the amount of reserves that is used for rewards each epoch

Governs the long-term sustainability of Cardano

- The reserves are gradually depleted until no rewards are supplied

Guardrails

ME-01 (y) *monetaryExpansion* **must not** exceed 0.005

ME-02 (y) *monetaryExpansion* **must not** be lower than 0.001

ME-03 (y) *monetaryExpansion* **must not** be negative

ME-04 (x - "should") *monetaryExpansion* **should not** be varied by more than +/- 10% in any 73-epoch period (approximately 12 months)

ME-05 (x - "should") *monetaryExpansion* **should not** be changed more than once in any 36-epoch period (approximately 6 months)

Plutus Script Execution Prices

(executionUnitPrices[priceSteps/priceMemory]) Define the fees for executing

Plutus scripts

Gives an economic return for Plutus script execution

Provides security against low-cost DoS attacks

Guardrails

EIUP-PS-01 (y) *executionUnitPrices[priceSteps]* **must not** exceed 2,000 / 10,000,000

EIUP-PS-02 (y) *executionUnitPrices[priceSteps]* **must not** be lower than 500 / 10,000,000

EIUP-PM-01 (y) *executionUnitPrices[priceMemory]* **must not** exceed 2,000 / 10,000

EIUP-PM-02 (y) *executionUnitPrices[priceMemory]* **must not** be lower than 400 /

10,000 EIUP-GEN-01 (x - "similar to") The execution prices **must** be set so that

i) the cost of executing a transaction with maximum CPU steps is similar to the cost of a maximum sized non-script transaction and
ii) the cost of executing a transaction with maximum memory units is similar to the cost of a maximum sized non-script transaction

EIUP-GEN-02 (x - "should") The execution prices **should** be adjusted whenever transaction fees are adjusted (*txFeeFixed/txFeePerByte*). The goal is to ensure that the processing delay is similar for "full" transactions, regardless of their type.

- This helps ensure that the requirements on block diffusion/propagation times are

met.

Transaction fee per byte for a reference script (minFeeRefScriptCoinsPerByte)

Defines the cost for using Plutus reference scripts in Lovelace

Guardrails

MFRS-01 (y) *minFeeRefScriptCoinsPerByte* **must not** exceed 1,000 (0.001 ada)
- This ensures that transactions can be paid for

MFRS-02 (y) *minFeeRefScriptCoinsPerByte* **must not** be negative

MFRS-03 (x - "should") To maintain a consistent level of protection against denial-of-service attacks, *minFeeRefScriptCoinsPerByte* **should** be adjusted whenever Plutus Execution prices are adjusted (*executionUnitPrices[steps/memory]*) and whenever *txFeeFixed* is adjusted

MFRS-04 (x - unquantifiable) Any changes to *minFeeRefScriptCoinsPerByte* **must** consider the implications of reducing the cost of a denial-of-service attack or increasing the

maximum transaction fee

2.3. Network Parameters

The overall goals when managing the Cardano Blockchain network parameters are to:

1. Match the available Cardano Blockchain Layer 1 network capacity to current or future traffic demands, including payment transactions, layer 1 DApps, sidechain management and governance needs
2. Balance traffic demands for different user groups, including payment transactions, minters of Fungible/Non-Fungible Tokens, Plutus scripts, DeFi developers, Stake Pool Operators and voting transactions

Triggers for Change

Changes to network parameters may be triggered by:

1. Measured changes in traffic demands over a 2-epoch period (10 days)
2. Anticipated changes in traffic demands
3. Community requests

Counter-indicators

Changes may need to be reversed and/or should not be enacted in the event of:

- Excessive block propagation delays
- Stake pools being unable to handle traffic volume
- Scripts being unable to complete execution

Core Metrics

All decisions on parameter changes should be informed by:

- Block propagation delay profile
- Traffic volume (block size over time)
- Script volume (size of scripts and execution units)
- Script execution cost benchmarks
- Block propagation delay/diffusion benchmarks

Detailed benchmarking results are required to confirm the effect of any changes on mainnet performance or behavior prior to enactment. The effects of different transaction mixes must be analyzed, including normal transactions, Plutus scripts, and governance actions.

Guardrails

NETWORK-01 (x - "should") No individual network parameter **should** change more than

once per two epochs

NETWORK-02 (x - "should") Only one network parameter **should** be changed per epoch unless they are directly correlated, e.g., per-transaction and per-block memory unit limits

Changes to Specific Network Parameters

Block Size (maxBlockBodySize)

The maximum size of a block, in Bytes.

Guardrails

MBBS-01 (y) *maxBlockBodySize* **must not** exceed 122,880 Bytes (120KB)

MBBS-02 (y) *maxBlockBodySize* **must not** be lower than 24,576 Bytes (24KB)

MBBS-03 (x - "exceptional circumstances") *maxBlockBodySize* **must not** be decreased, other than in exceptional circumstances where there are potential problems with security, performance, ~~or~~ functionality or long-term sustainability

MBBS-04 (~ - no access to existing parameter values) *maxBlockBodySize* **must** be large enough to include at least one transaction (that is, *maxBlockBodySize* **must** be at least *maxTxSize*)

MBBS-05 (x - "should") *maxBlockBodySize* **should** be changed by at most 10,240 Bytes (10KB) per epoch (5 days), and preferably by 8,192 Bytes (8KB) or less per epoch

MBBS-06 (x - "should") The block size **should not** induce an additional Transmission Control Protocol (TCP) round trip. Any increase beyond this must be backed by performance analysis, simulation and benchmarking

MBBS-07 (x - "unquantifiable") The impact of any change to *maxBlockBodySize* **must** be confirmed by detailed benchmarking/simulation and not exceed the requirements of the block diffusion/propagation time budgets, as described below. Any increase to *maxBlockBodySize* must also consider future requirements for Plutus script execution (*maxBlockExecutionUnits[steps]*) against the total block diffusion target of 3s with 95% block propagation within 5s. The limit on maximum block size may be increased in the future if this is supported by benchmarking and monitoring results

Transaction Size (maxTxSize)

The maximum size of a transaction, in Bytes.

Guardrails

MTS-01 (y) *maxTxSize* **must not** exceed 32,768 Bytes (32KB)

MTS-02 (y) *maxTxSize* **must not** be negative

MTS-03 (~ - no access to existing parameter values) *maxTxSize* **must not** be decreased

MTS-04 (~ - no access to existing parameter values) *maxTxSize* **must not** exceed *maxBlockBodySize*

MTS-05 (x - "should") *maxTxSize* **should not** be increased by more than 2,560 Bytes (2.5KB) in any epoch, and preferably **should** be increased by 2,048 Bytes (2KB) or less per epoch

MTS-06 (x - "should") *maxTxSize* **should not** exceed 1/4 of the block size

Memory Unit Limits (maxBlockExecutionUnits[memory],

maxTxExecutionUnits[memory])

The limit on the maximum number of memory units that can be used by Plutus scripts, either per-transaction or per-block.

Guardrails

MTEU-M-01 (y) *maxTxExecutionUnits[memory]* **must not** exceed 40,000,000

units

MTEU-M-02 (y) *maxTxExecutionUnits[memory]* **must not** be negative

MTEU-M-03 (~ - no access to existing parameter values) *maxTxExecutionUnits[memory]* **must not** be decreased

MTEU-M-04 (x - "should") *maxTxExecutionUnits[memory]* **should not** be increased by more than 2,500,000 units in any epoch

MBEU-M-01 (y) *maxBlockExecutionUnits[memory]* **must not** exceed 120,000,000 units
MBEU-M-02 (y) *maxBlockExecutionUnits[memory]* **must not** be negative

MBEU-M-03 (x - "should") *maxBlockExecutionUnits[memory]* **should not** be changed (increased or decreased) by more than 10,000,000 units in any epoch

MBEU-M-04 (x - unquantifiable) The impact of any change to *maxBlockExecutionUnits[memory]* **must** be confirmed by detailed benchmarking/simulation and not exceed the requirements of the block diffusion/propagation time budgets, as also impacted by *maxBlockExecutionUnits[steps]* and *maxBlockBodySize*. Any increase **must** also consider previously agreed future requirements for the total block size (*maxBlockBodySize*) measured against the total block diffusion target of 3s with 95% block propagation within 5s. Future Plutus performance improvements may allow the per-block memory limit to be increased, but must be balanced

against the overall diffusion limits as specified in the previous sentence, and future requirements

MEU-M-01 (~ - no access to existing parameter values) *maxBlockExecutionUnits[memory]* **must not** be less than *maxTxExecutionUnits[memory]*

CPU Unit Limits (maxBlockExecutionUnits[steps], maxTxExecutionUnits[steps])

The limit on the maximum number of CPU steps that can be used by Plutus scripts, either per transaction or per-block.

Guardrails

MTEU-S-01 (y) *maxTxExecutionUnits[steps]* **must not** exceed 15,000,000,000 (15Bn) units

MTEU-S-02 (y) *maxTxExecutionUnits[steps]* **must not** be negative

MTEU-S-03 (~ - no access to existing parameter values) *maxTxExecutionUnits[steps]* **must not** be decreased

MTEU-S-04 (x - "should") *maxTxExecutionUnits[steps]* **should not** be increased by more than 500,000,000 (500M) units in any epoch (5 days)

MBEU-S-01 (y) *maxBlockExecutionUnits[steps]* **must not** exceed 40,000,000,000 (40Bn) units

MBEU-S-02 (y) *maxBlockExecutionUnits[steps]* **must not** be negative

MBEU-S-03 (x - "should") *maxBlockExecutionUnits[steps]* **should not** be changed (increased or decreased) by more than 2,000,000,000 (2Bn) units in any epoch (5 days)

MBEU-S-04 (x - unquantifiable) The impact of the change to *maxBlockExecutionUnits[steps]* **must** be confirmed by detailed benchmarking/simulation and not exceed the requirements of the block diffusion/propagation time budgets, as also impacted by *maxBlockExecutionUnits[memory]* and *maxBlockBodySize*. Any increase **must** also consider previously identified future requirements for the total block size (*maxBlockBodySize*) measured against the total block diffusion target of 3s with 95% block propagation within 5s. Future Plutus performance improvements may allow the per-block step limit to be increased, but **must** be balanced against the overall diffusion limits as specified in the previous sentence, and future requirements

MEU-S-01 (~ - no access to existing parameter values) *maxBlockExecutionUnits[steps]* **must not** be less than *maxTxExecutionUnits[steps]*

Block Header Size (maxBlockHeaderSize)

The size of the block header.

~~Note that increasing the block header size may affect the overall block size (*maxBlockBodySize*)~~

Guardrails

MBHS-01 (y) *maxBlockHeaderSize* **must not** exceed 5,000

Bytes MBHS-02 (y) *maxBlockHeaderSize* **must not** be negative

MBHS-03 (x - "largest valid header" is subject to change) *maxBlockHeaderSize* **must** be large enough for the largest valid header

MBHS-04 (x - "should") *maxBlockHeaderSize* **should** only normally be increased if the protocol changes

MBHS-05 (x - "should") *maxBlockHeaderSize* **should** be within TCP's initial congestion window (3 or 10 MTUs)

2.4. Technical/Security Parameters

The overall goals when managing the technical/security parameters are:

1. Ensure the security of the Cardano network in terms of decentralization, protection against Sybil and 51% attacks and protection against denial of service attacks

2. Enable changes to the Plutus language

Triggers for Change

1. Changes in the number of active SPOs
2. Changes to the Plutus language
3. Security threats
4. Community requests

Counter-indicators

- Economic concerns, e.g. when changing the number of stake pools

Core Metrics

- Number of stake pools
- Level of decentralization

Changes to Specific Technical/Security Parameters

Target Number of Stake Pools (stakePoolTargetNum)

Sets the target number of stake pools

- The expected number of pools when the network is in the equilibrium state
- Primarily a security parameter, ensuring decentralization by pool division/replication
- Has an economic effect as well as a security affect - economic advice is also required when changing this parameter
- Large changes in this parameter will trigger mass redelegation events

Guardrails

SPTN-01 (y) *stakePoolTargetNum* **must not** be lower than 250

SPTN-02 (y) *stakePoolTargetNum* **must not** exceed 2,000

SPTN-03 (y) *stakePoolTargetNum* **must not** be negative

SPTN-04 (y) *stakePoolTargetNum* **must not** be zero

Pledge Influence Factor (poolPledgeInfluence)

Enables the pledge protection mechanism

Provides protection against Sybil attack

- Higher values reward pools that have more pledge and penalize pools that have less pledge

Has an economic effect as well as technical effect - economic advice is also required

~~- Can be set in the range 0.0-infinity~~

Guardrails

PPI-01 (y) *poolPledgeInfluence* **must not** be lower than 0.1

PPI-02 (y) *poolPledgeInfluence* **must not** exceed 1.0

PPI-03 (y) *poolPledgeInfluence* **must not** be negative

PPI-04 (x - "should") *poolPledgeInfluence* **should not** vary by more than +/- 10% in any 18-epoch period (approximately 3 months)

Pool Retirement Window (poolRetireMaxEpoch)

Defines the maximum number of epochs notice that a pool can give when planning to

retire

Guardrails

PRME-01 (y) *poolRetireMaxEpoch* **must not** be negative

PRME-02 (x - "should") *poolRetireMaxEpoch* **should not** be lower than

1 *Collateral Percentage (collateralPercentage)*

Defines how much collateral must be provided when executing a Plutus script as a percentage of the normal execution cost

- Collateral is additional to fee payments
- If a script fails to execute, then the collateral is lost
- The collateral is never lost if a script executes successfully

Provides security against low-cost attacks by making it more expensive rather than less expensive to execute failed scripts

Guardrails

CP-01 (y) *collateralPercentage* **must not** be lower than 100

CP-02 (y) *collateralPercentage* **must not** exceed 200

CP-03 (y) *collateralPercentage* **must not** be negative

CP-04 (y) *collateralPercentage* **must not** be zero

Maximum number of collateral inputs (maxCollateralInputs)

Defines the maximum number of inputs that can be used for collateral when executing a Plutus script

Guardrails

MCI-01 (y) *maxCollateralInputs* **must not** be lower than 1

Maximum Value Size (maxValueSize)

The limit on the serialized size of the Value in each output.

Guardrails

MVS-01 (y) *maxValueSize* **must not** exceed 12,288 Bytes

(12KB) MVS-02 (y) *maxValueSize* **must not** be negative

MVS-03 (~ - no access to existing parameter values) *maxValueSize* **must** be less than *maxTxSize*

MVS-04 (~ - no access to existing parameter values) *maxValueSize* **must not** be reduced

MVS-05 (x - "sensible output" is subject to interpretation) *maxValueSize* **must** be large enough to allow sensible outputs (e.g. any existing on-chain output or anticipated outputs that could be produced by new ledger rules)

Plutus Cost Models (costModels)

Define the base costs for each Plutus primitive in terms of CPU and memory unit

A different cost model is required for each Plutus version. Each cost model comprises many distinct cost model values
~~- There are about 150 distinct micro-parameters in total~~

Cost models are defined for each Plutus language version. A new language version may introduce additional micro-parameters or remove existing micro-parameters.

Guardrails

PCM-01 (x - unquantifiable) *Cost model* values **must** be set by benchmarking on a reference architecture

PCM-02 (x - primitives and language versions aren't introduced in transactions) The *cost model* **must** be updated if new primitives are introduced or a new Plutus language version is added

PCM-03 (~ - no access to *Plutus cost model* parameters) *Cost model* values **should not** normally be negative. Negative values must be justified against the underlying cost model for the associated primitives.

PCM-04 (~ - no access to *Plutus cost model* parameters) A *cost model* **must** be supplied for each Plutus language version that the protocol supports

2.5. Governance Parameters

The overall goals when managing the governance parameters are to:

1. Ensure governance stability
2. Maintain a representative form of governance ~~as outlined in CIP-1694~~

Triggers for Change

Changes to governance parameters may be triggered by:

1. Community requests
2. Regulatory requirements
3. Unexpected or unwanted governance outcomes
4. Entering a state of no confidence

Counter-indicators

Changes may need to be reversed and/or should not be enacted in the event of:

- Unexpected effects on governance
- Excessive Layer 1 load due to on-chain voting or excessive numbers of governance actions

Core Metrics

All decisions on parameter changes should be informed by:

- Governance participation levels
- Governance behaviors and patterns
- Regulatory considerations
- Confidence in the governance system
- The effectiveness of the governance system in managing necessary

change *Changes to Specific Governance Parameters*

Deposit for Governance Actions (govDeposit)

The deposit that is charged when submitting a governance action.

- Helps to limit the number of actions that are submitted

Guardrails

GD-01 (y) *govDeposit* **must not** be negative

GD-02 (y) *govDeposit* **must not** be lower than 1,000,000 (1 ada)

GD-03 (y) *govDeposit* **must not** exceed 10,000,000,000,000 (10 Million ada)

GD-04 (x - "should") *govDeposit* **should** be adjusted in line with fiat changes

Deposit for DReps (dRepDeposit)

The deposit that is charged when registering a DRep.

- Helps to limit the number of active DReps

Guardrails

DRD-01 (y) *dRepDeposit* **must not** be negative

DRD-02 (y) *dRepDeposit* **must not** be lower than 1,000,000 (1 ada) DRD-03

(y) *dRepDeposit* **must not** exceed 100,000,000,000 (100,000 ada) DRD-04 (x -

"should") *dRepDeposit* **should** be adjusted in line with fiat changes *DRep*

Activity Period (dRepActivity)

The period (as a whole number of epochs) after which a DRep is considered to be inactive for vote calculation purposes, if they do not vote on any proposal.

Guardrails

DRA-01 (y) *dRepActivity* **must not** be lower than 13 epochs (2 months)

DRA-02 (y) *dRepActivity* **must not** exceed 37 epochs (6 months)

DRA-03 (y) *dRepActivity* **must not** be negative

DRA-04 (~ - no access to existing parameter values) *dRepActivity* **must** be greater than *govActionLifetime*

DRA-05 (x - "should") *dRepActivity* **should** be calculated in human terms (2 months etc)

DRep and SPO Governance Action Thresholds

dRepVotingThresholds[...],poolVotingThresholds[...])

Thresholds on the active voting stake that is required to ratify a specific type of governance action by either DReps or SPOs.

- Ensures legitimacy of the action

The threshold parameters are listed below:

dRepVotingThresholds:

- *dvtCommitteeNoConfidence*
- *dvtCommitteeNormal*
- *dvtHardForkInitiation*
- *dvtMotionNoConfidence*

- *dvtPPEconomicGroup*
- *dvtPPGovGroup*
- *dvtPPNetworkGroup*
- *dvtPPTechnicalGroup*
- *dvtTreasuryWithdrawal*
- *dvtUpdateToConstitution*

poolVotingThresholds:

- *pvtCommitteeNoConfidence*
- *pvtCommitteeNormal*
- *pvtHardForkInitiation*
- *pvtMotionNoConfidence*
- *pvtPPSecurityGroup*

Guardrails

VT-GEN-01 (y) All thresholds **must** be greater than 50% and less than or equal to 100%

VT-GEN-02 (y) Economic, network and technical parameter thresholds **must** be in the range 51%-75%

VT-GEN-03 (y) Governance parameter thresholds **must** be in the range

75%-90% VT-HF-01 (y) **Hard fork** action thresholds **must** be in the range

51%-80%

VT-CON-01 (y) **New Constitution or guardrails script action** thresholds **must** be in the range 65%-90%

VT-CC-01 (y) **Update Constitutional Committee action** thresholds **must** be in the range 51%-90%

VT-NC-01 (y) **No confidence** action thresholds **must** be in the range 51%-75%

Governance Action Lifetime (govActionLifetime)

The period after which a governance action will expire if it is not

enacted - As a whole number of epochs

Guardrails

GAL-01 (y) *govActionLifetime* **must not** be lower than 1 epoch (5 days)

GAL-03 (x - "should") *govActionLifetime* **should not** be lower than 2 epochs (10

days)

GAL-02 (y) *govActionLifetime* **must not** exceed 15 epochs (75 days)

GAL-04 (x - "should") *govActionLifetime* **should** be calibrated in human terms (eg 30 days, two weeks), to allow sufficient time for voting etc. to take place

GAL-05 (~ - no access to existing parameter values) *govActionLifetime* **must** be less than *dRepActivity*

Maximum Constitutional Committee Term (committeeMaxTerm~~Limit~~Length)

The limit on the maximum term length that a committee member may serve

Guardrails

CMTL-01 (y) *committeeMaxTerm~~Limit~~Length* **must not** be zero

CMTL-02 (y) *committeeMaxTerm~~Limit~~Length* **must not** be negative

CMTL-03 (y) *committeeMaxTerm~~Limit~~Length* **must not** be lower than 18 epochs (90 days, or approximately 3 months)

CMTL-04 (y) *committeeMaxTerm~~Limit~~Length* **must not** exceed 293 epochs (approximately 4 years)

CMTL-05 (x - "should") *committeeMaxTerm~~Limit~~Length* **should not** exceed 220 epochs (approximately 3 years)

The minimum size of the Constitutional Committee (committeeMinSize)

The least number of members that can be included in a Constitutional Committee following a governance action to change the Constitutional Committee.

Guardrails

CMS-01 (y) *committeeMinSize* **must not** be negative

CMS-02 (y) *committeeMinSize* **must not** be lower than 3

CMS-03 (y) *committeeMinSize* **must not** exceed 10

2.6. Monitoring and Reversion of Parameter Changes

All network parameter changes **must be** monitored carefully for no less than 2 epochs (10 days)

- Changes **must** be reverted as soon as possible if block propagation delays exceed 4.5s for more than 5% of blocks over any 6 hour rolling window

All other parameter changes should be monitored

- The reversion plan **should** be implemented if the overall effect on performance, security, ~~or~~ functionality or long-term sustainability is unacceptable.

A specific reversion/recovery plan **must be** produced for each parameter change. This plan must include:

- Which parameters need to change and in which ways in order to return to the previous state (or a similar state)
- How to recover the network in the event of disastrous failure

This plan **should** be followed if problems are observed following the parameter change. Note that not all changes can be reverted. Additional care must be taken when making changes to these parameters.

2.7. Non-Updatable Protocol Parameters

Some fundamental protocol parameters cannot be changed by the Protocol Parameter Update governance action. These parameters can only be changed in a new Genesis file as part of a hard fork. It is not necessary to provide specific guardrails on updating these parameters.

3. GUARDRAILS AND GUIDELINES ON TREASURY WITHDRAWAL ACTIONS

Treasury withdrawal actions specify the destination and amount of a number of withdrawals from the Cardano treasury.

Guardrails

TREASURY-01 (x) ~~DReps **must** define a net change limit for the Cardano Treasury's balance per period of time.~~ [A net change limit for the Cardano Treasury's balance per period of time **must** be agreed by the DReps via an on-chain governance action with a threshold of greater than 50% of the active voting stake.] *[[Under discussion]]*

TREASURY-02 (x) The budget for the Cardano Treasury **must not** exceed the net change limit for the Cardano Treasury's balance per period of time.

TREASURY-03 (x) The budget for the Cardano Treasury **must** be denominated in ada.

TREASURY-04 (x) Treasury withdrawals **must not** be ratified until there is a community approved Cardano budget then in effect pursuant to a previous on-chain governance action agreed by the DReps with a threshold of greater than 50% of the active voting stake.

4. GUARDRAILS AND GUIDELINES ON HARD FORK INITIATION ACTIONS

The **hard fork initiation** action requires both a new major and a new minor protocol version to be specified.

- As positive integers

As the result of a hard fork, new updatable protocol parameters may be introduced. Guardrails may be defined for these parameters, which will take effect following the hard fork. Existing updatable protocol parameters may also be deprecated by the hard fork, in which case the guardrails become obsolete for all future changes.

Guardrails

HARDFORK-01 (~ - no access to existing parameter values) The major protocol version **must** be the same as or one greater than the major version that will be enacted immediately prior to this change. If the major protocol version is one greater, then the minor protocol version **must** be zero.

HARDFORK-02 (~ - no access to existing parameter values) ~~The minor protocol version **must** be no less than the minor version that will be enacted immediately prior to this change.~~ Unless the major protocol version is also changed, the minor protocol version **must** be greater than the minor version that will be enacted immediately prior to this change.

HARDFORK-03 (~ - no access to existing parameter values) At least one of the protocol versions (major or minor or both) **must** change.

HARDFORK-04 (x) At least 85% of stake pools by active stake **should** have upgraded to a Cardano node version that is capable of processing the rules associated with the new protocol version.

HARDFORK-05 (x) Any new updatable protocol parameters that are introduced with a hard fork **must** be included in this Appendix and suitable guardrails defined for those parameters.

HARDFORK-06 (x) Settings for any new protocol parameters that are introduced with a hard fork **must** be included in the appropriate Genesis file.

HARDFORK-07 (x) Any deprecated protocol parameters **must** be indicated in this Appendix.

HARDFORK-08 (~ - no access to *Plutus cost model* parameters) New Plutus versions **must** be supported by a version-specific *Plutus cost model* that covers each primitive that is available in the new Plutus version.

5. GUARDRAILS AND GUIDELINES ON UPDATE CONSTITUTIONAL COMMITTEE OR THRESHOLD ACTIONS

Update Constitutional Committee or Threshold governance actions may change the size, composition or required voting thresholds for the Constitutional Committee

Guardrails

UPDATE-CC-01 (x) **Update Constitutional Committee and/or threshold** **and/or term** governance actions **must not** be ratified until ada holders have ratified through an on-chain governance action this ~~the Final~~ Constitution.

6. GUARDRAILS AND GUIDELINES ON NEW CONSTITUTION OR GUARDRAILS SCRIPT ACTIONS

New constitution or guardrails script actions change the hash of the on-chain constitution and the associated guardrails script.

Guardrails

NEW-CONSTITUTION-01 (x) An **New Constitution** **or Guardrails Script** governance action **must** be submitted to define any required guardrails for new parameters that are introduced via a Hard Fork governance action

NEW-CONSTITUTION-02 (x) If specified, the new guardrails script must be consistent with this Constitution.

7. GUARDRAILS AND GUIDELINES ON NO CONFIDENCE ACTIONS

No confidence actions signal a state of no confidence in the governance system. No guardrails are imposed on **No Confidence** actions.

Guardrails

- None

8. GUARDRAILS AND GUIDELINES ON INFO ACTIONS

Info actions are not enacted on-chain. No guardrails are imposed on **Info**

actions. ***Guardrails***

- None

9. GUARDRAILS DURING THE INTERIM PERIOD

DEPRECATED

~~*Interim Period*~~

~~The Interim Period begins with the Chang Hard-Fork and ends after a community-ratified Final~~

Constitution is enacted on-chain. Throughout the Interim Period, technical and constitution enforced triggers will progressively turn on the features of CIP-1694.

I*nterim Period Technical Rollout:*

- The Chang Hard Fork will enable three initial CIP-1694 governance actions and enable the representative framework to be established.

These actions are the **"Info"**, **"Hard-fork initiation"** and **"Protocol parameter changes"** actions.

ada holders will be able to register as and delegate to DReps immediately after the hard fork but, as described in CIP-1694, DRep voting will not be available, except on **"Info"** actions. This ensures that ada holders have sufficient time to choose their voting delegations.

SPOs will be able to vote as described in CIP-1694.

"Hard-fork initiation" and **"Protocol parameter changes"** actions will also be ratified by the Constitutional Committee.

ada holders will be able to withdraw their staking rewards as usual.

- A subsequent hard fork, ratified by the Constitutional Committee and SPOs, shortly after the Chang Hard Fork, will enable the four remaining CIP-1694 governance actions:

"treasury withdrawals",
"motion of no-confidence",
"update constitutional committee and/or threshold and/or terms",
and **"new constitution or guardrails script"**.

At this point, DRep voting will be enabled and staking rewards can only be withdrawn if the ada holder has delegated their vote (including to the pre-defined Abstain/No Confidence voting options).

Guardrails

INTERIM-01 (x) To provide sufficient time for DReps to register and campaign and for ada holders to choose their initial voting delegations, at least 18 epochs (90 days, or approximately 3 months) **must** elapse after the Chang hard fork before the subsequent hard fork can be ratified. Once the subsequent hard fork is enacted, DRep voting can occur as described in CIP 1694.

INTERIM-02 (x) Treasury withdrawals **must not** be ratified until there is a community approved Cardano Blockchain Ecosystem budget then in effect pursuant to a previous on-chain governance action.

INTERIM-03 (x) Treasury withdrawals **must** be consistent with the community-approved Cardano Blockchain ecosystem budget(s).

~~INTERIM-04 (x) ada holders **must** have ratified the Final Constitution as specified in Appendix II before ratifying any other proposed **"new constitution"**, **"update constitutional committee**, **and/or threshold and/or terms"**, and **"motion of no confidence"** governance actions.~~

~~INTERIM-05 (x) **"New guardrails script"** actions that are consistent with the Interim Constitution may be ratified during the interim period, provided the Interim Constitution itself is not changed.~~

10. LIST OF PROTOCOL PARAMETER GROUPS

The protocol parameters are grouped by type, allowing different thresholds to be set for each group.

The network group consists of:

- *maximum block body size* (*maxBlockBodySize*)
- *maximum transaction size* (*maxTxSize*)
- *maximum block header size* (*maxBlockHeaderSize*)
- *maximum size of a serialized asset value* (*maxValueSize*)
- *maximum script execution units in a single transaction* (*maxTxExecutionUnits[steps]*)
- *maximum script execution units in a single block* (*maxBlockExecutionUnits[steps]*)
- *maximum number of collateral inputs* (*maxCollateralInputs*)

The economic group consists of:

- *minimum fee coefficient* (*txFeePerByte*)
- *minimum fee constant* (*txFeeFixed*)
- *minimum fee per byte for reference scripts* (*minFeeRefScriptCoinsPerByte*) - *delegation key Lovelace deposit* (*stakeAddressDeposit*)
- *pool registration Lovelace deposit* (*stakePoolDeposit*)
- *monetary expansion* (*monetaryExpansion*)
- *treasury expansion* (*treasuryCut*)
- *minimum fixed rewards cut for pools* (*minPoolCost*)
- *minimum Lovelace deposit per byte of serialized UTxO* (*coinsPerUTxOByte*) - *prices of Plutus execution units* (*executionUnitPrices[priceSteps/priceMemory]*)

The technical group consists of:

- *pool pledge influence* (*poolPledgeInfluence*)
- *pool retirement maximum epoch* (*poolRetireMaxEpoch*)
- *desired number of pools* (*stakePoolTargetNum*)
- *Plutus execution cost models* (*costModels*)

- *proportion of collateral needed for scripts* (*collateralPercentage*)

The governance group consists of all the new protocol parameters ~~that are introduced in CIP 1694~~:

- *governance voting thresholds* (*dRepVotingThresholds[...], poolVotingThresholds[...]*)
- *governance action maximum lifetime in epochs* (*govActionLifetime*) - *governance action deposit* (*govActionDeposit*)
- *DRep deposit amount* (*dRepDeposit*)
- *DRep activity period in epochs* (*dRepActivity*)
- *minimal constitutional committee size* (*committeeMinSize*)
- *maximum term length (in epochs) for the constitutional committee members* (*committeeMaxTerm~~Limit~~Length*)