CARDANO BLOCKCHAIN ECOSYSTEM CONSTITUTION

PREAMBLE

Cardano is a decentralized ecosystem of blockchain technology, smart contracts, and community governance, committed to improving economic, political, and social systems for everyone, everywhere. By offering this foundational infrastructure, Cardano empowers individuals and communities to manage their identity, value and governance, fostering the emergence of decentralized applications, businesses and network states.

Through unbiased processing of immutable data, we the participants of the Cardano Community, consisting of individuals, organizations, contributors and others, choose to follow in the footsteps of the early Internet and cryptocurrency pioneers, who first forged bonds of community through digital technologies. We are guided by our shared principles and tenets as we exercise our self-governance by balancing decentralized decision-making with accountability and safeguarding the security of the Cardano Blockchain.

Recognizing the need for a more robust and dynamic governance framework, that neither relies nor depends upon traditional nation-state governance systems, but instead relies on self-governance by the Cardano Community, utilizing, wherever possible and beneficial, blockchain technology in the governance process, we hereby establish this Cardano Constitution to govern the Cardano Blockchain ecosystem, ensure the continuity of the Cardano Blockchain, and guard the rights of those who utilize it.

With these purposes in mind, we the Cardano Community affirm our intention to abide by this Constitution in order to participate in the governance of the Cardano Blockchain ecosystem. We invite all who share our values to join us but stand not in the way of any who wish to take another path.

ARTICLE I. CARDANO BLOCKCHAIN TENETS AND GUARDRAILS

Section 1

These below Tenets shall guide all participants of the Cardano Community, including the Constitutional Committee, and proposed governance actions shall be evaluated in accordance with these Tenets. The order in which the below Tenets appear is not intended to represent a priority among Tenets.

TENET 1 Transactions on the Cardano Blockchain shall not be slowed down or censored and shall be expediently served for their intended purpose.

TENET 2 The cost of transactions on the Cardano Blockchain shall be predictable and not unreasonable.

TENET 3 Anyone desiring to develop and deploy applications on the Cardano Blockchain shall not unreasonably be prevented from developing and deploying such applications as intended.

TENET 4 Contributions by the Cardano Community on the Cardano Blockchain shall be recognized, recorded and assessed fairly through reward sharing with SPOs, potential compensation to DReps and CC members, and appropriate tokenomics.

TENET 5 The Cardano Blockchain shall not lock in an ada owner's value or data without the owner's consent.

TENET 6 The Cardano Blockchain shall not unreasonably impede interoperability.

TENET 7 The Cardano Blockchain shall preserve in a safe manner any value and information stored on the Cardano Blockchain.

TENET 8 The Cardano Blockchain shall not unreasonably spend resources.

TENET 9 All users of the Cardano Blockchain shall be treated equitably, taking into account the collective desires of the Cardano Blockchain Community, consistent with the long-term sustainability and viability of the Cardano Blockchain.

TENET 10 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).

Section 2

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

In the event there are inconsistencies between a Guardrail as set forth in the Cardano Blockchain Guardrails Appendix and any such Guardrail that has been programmed and implemented on the Cardano Blockchain, the version of such Guardrail that has been deployed directly on the Cardano Blockchain shall prevail unless and until replaced or revised pursuant to an on-chain governance action. TheConstitutional 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 considered to be participants in the Cardano Community and are therefore recognized as beneficiaries of the Cardano Blockchain ecosystem. All participants in the Cardano Community 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

Participants in the Cardano Community who own ada 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 actions regarding the Cardano Blockchain.

Section 3

The Cardano Community has a responsibility to maintain the integrity of the Cardano Blockchain ecosystem by following this Constitution, operating the Cardano Blockchain, 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 Blockchain, and to form temporary and permanent organizations, associations and other entities as the Cardano Community deems desirable or appropriate in support of the Cardano Blockchain ecosystem.

ARTICLE III. PARTICIPATORY AND DECENTRALIZED GOVERNANCE

Section 1

The Cardano Blockchain 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 this Constitution, including the Cardano Blockchain Guardrails Appendix. On-chain governance actions shall be effected through a collective decision-making process, with specific consensus threshold requirements, as required by 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 (DReps), Stake Pool Operators (SPOs) and the Constitutional Committee (CC).

Section 3

All owners of ada shall have the right to vote in on-chain governance decision-making processes, as provided for in this Constitution and the Cardano Blockchain Guardrails Appendix. All owners of ada shall have the right to propose changes to the governance structure of the Cardano Blockchain ecosystem in accordance with the 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.

Section 4

A special form of on-chain governance action, an “Info” action, exists to allow the Cardano Community to propose potential future on-chain governance actions and to allow community sentiment to be gauged without committing to any on-chain change of the Cardano Blockchain. Such "Info" actions have no on-chain effect other than to record such “Info” action on the Cardano Blockchain. “Info” action may also be used to seek approval for proposed Cardano Blockchain ecosystem budgets and Cardano Blockchain treasury withdrawals.

Section 5

In order to promote transparency in the process of on-chain governance, prior to being recorded or enacted on-chain, all proposed governance actions are expected to follow a standardized and legible format including a URL and hash of all documented off-chain content to the Cardano Blockchain. 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.

The content of every on-chain governance action must be identical to the final off-chain version of the proposed action.

“Hard Fork Initiation” and “Protocol Parameter Change” governance actions shall undergo sufficient technical review and scrutiny as mandated by the Guardrails to ensure that the governance action does not endanger the security, functionality, 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 6

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.

ARTICLE IV. THE CARDANO BLOCKCHAIN ECOSYSTEM BUDGET

Section 1

Any participant in the Cardano Community may propose a Cardano Blockchain ecosystem budget at any time. The Cardano Community is expected to periodically propose one or more budgets for the ongoing operation, maintenance and future development of the Cardano Blockchain ecosystem and for covering other costs related to the implementation, administration and maintenance of the decentralized, on-chain governance processes provided for in this Constitution. The Cardano Community may propose one aggregate budget or multiple budgets for the Cardano Blockchain ecosystem. Such budgets are expected to cover not less than a period of 73 epochs (approximately one calendar year) but nothing shall prevent the Cardano Community from proposing budgets for shorter or longer time periods. All owners of ada are expected to periodically approve one or more Cardano Blockchain ecosystem budgets through an on-chain "Info" action. As provided in Section 3 of this Article IV, withdrawals may be made from the Cardano Blockchain treasury as necessary from time to time to give effect to the Cardano Blockchain ecosystem budget or budgets then in effect. Existing budgets may be amended following the same process as provided in this Section 1.

Section 2

Development of Cardano Blockchain ecosystem budgets and the administration of such budgets shall utilize, to the extent possible and beneficial, smart contracts and other blockchain based tools to facilitate decision-making and ensure transparency. 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.

Section 3

Withdrawals from the Cardano Blockchain treasury that would cause the Cardano Blockchain treasury balance to violate the then applicable net change limit shall not be permitted. No withdrawals from the Cardano Blockchain treasury shall be permitted unless such withdrawals have been authorized and are being made pursuant to a budget for the Cardano Blockchain that is then in effect as required by the Cardano Blockchain Guardrails Appendix, and which has not been determined by the Constitutional Committee to be unconstitutional.

Section 4

Any governance action requesting ada from the Cardano Blockchain treasury 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 Blockchain ecosystem budget shall include dispute resolution provisions.

Section 5

Any ada received from a Cardano Blockchain treasury withdrawal, so long as such ada is being held directly or indirectly by an administrator prior to further disbursement, must be kept in one or more separate accounts that can be audited by the Cardano Community, and such accounts may not be delegated to an SPO but must be delegated to the predefined auto abstain voting option.

ARTICLE V. 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. Owners of ada 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 the voting rights of the ada owner to registered DReps on the owner's behalf. DReps are entitled to cast votes directly for on-chain governance actions and represent those ada owners delegating their voting rights to them. DRep voting thresholds are set forth in the Cardano Blockchain Guardrails Appendix.

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

Section 3

DReps who are representing delegators are expected to periodically adopt, and update as they deem appropriate, codes of conduct governing their activities as DReps and make such codes of conduct publicly available. DReps are encouraged to include ethical guidelines in their codes of conduct.

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, access and evaluate DRep codes of conduct and select DReps on such criteria as they deem relevant.

Section 5

DReps who are representing delegators may be compensated for their efforts. DReps shall ensure that any compensation received in connection with their activities as a DRep is disclosed.

Section 6

DReps shall not pay compensation to an ada owner or to an owner's designee in exchange for being appointed a DRep by such ada owner or by its designee or for voting on behalf of such ada owner or its designee.

ARTICLE VI. 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 Appendix. 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 shall 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 and/or term" governance actions, and on "Parameter Update" governance actions that affect security-critical parameters set forth in the Cardano Blockchain Guardrails Appendix.

Section 3

SPOs are encouraged to periodically adopt, and update as they deem appropriate, codes of conduct governing their activities as SPOs and make such codes of conduct publicly available. SPOs are encouraged to include ethical guidelines in their codes of conduct.

Section 4

Owners of ada who are both SPOs and acting as DReps shall publicly disclose that they are

participating in on-chain governance actions in both such capacities prior to exercising any on-chain governance rights.

ARTICLE VII. CONSTITUTIONAL COMMITTEE

Section 1

A Constitutional Committee shall be established as the branch of Cardano's on-chain governance process that ensures governance actions to be enacted on-chain are consistent with this Constitution. The Constitutional Committee shall comprise a set of owners of ada that is collectively responsible for ensuring that on-chain governance actions prior to enactment on chain, are constitutional. Except as otherwise provided in Section 4 of this Article VII, the Constitutional Committee shall be limited to voting on the constitutionality of governance actions to be enacted on-chain. 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 sufficient to assure the ongoing integrity of the Cardano Blockchain as determined from time to time by owners of ada. The minimum and maximum number of members of the Constitutional Committee shall be consistent with the minimum and maximum number of members as set forth in the Cardano Blockchain Guardrails Appendix.

Members of the Constitutional Committee shall serve such term lengths as shall be determined from time to time by owners of ada as consistent with the minimum and maximum term lengths as set forth in the Cardano Blockchain Guardrails Appendix. To assure continuity in the operation of the Constitutional Committee, the terms for Constitutional Committee members shall be staggered.

Section 3

The Cardano Community shall establish and make public a process from time to time for election of members of the Constitutional Committee consistent with the requirements of the Guardrails.

Section 4

No governance action, other than a "Motion of no-confidence," or "Update Constitutional Committee/threshold and/or term” may be implemented on-chain unless a requisite percentage of the members of the Constitutional Committee as specified by the Guardrails shall have first determined and affirmed through an on-chain action that such proposal does not violate this Constitution. Each Constitutional Committee member shall have one vote.

Because “Info” actions have no on-chain effect and, accordingly, are neither constitutional nor

unconstitutional, Constitutional Committee members may not prevent “Info” actions from being recorded on-chain. Members of the Constitutional Committee may nevertheless record a vote on-chain regarding an “Info” action in order to express their view on such “Info” action, including whether the suggested course of action proposed in such “Info” action, would be, in the view of such member, unconstitutional if it were to be enforced by on-chain mechanisms.

In the case of “Info” actions that propose a Cardano Blockchain ecosystem budget, Constitutional Committee members shall record a vote on-chain that sets forth their opinion as to whether the proposed budget, if it were to be implemented in the form contained in the “Info” action, would violate this Constitution.

In the case of “Info” actions that propose a withdrawal from the Cardano Blockchain treasury pursuant to a previously approved budget, Constitutional Committee members shall record a vote on-chain that sets forth their opinion as to whether such proposed withdrawal, if made in accordance with such “Info” action, would violate this Constitution.

Section 5

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, other than “Info” actions, may go forward. During a state of no-confidence, “Info” actions other than “Info” actions relating to budget proposals or treasury withdrawal proposals, may continue to be recorded on-chain.

If a member of the Constitutional Committee is not carrying out its responsibilities as required by this Constitution, as so determined by a requisite percentage as specified by the Guardrails of SPOs and DReps, voting separately pursuant to an "Update Constitutional Committee/threshold and/or term" governance action, such member shall be removed from the Constitutional Committee upon the implementation of the governance action. Thereafter, an election shall be held as soon as practical to replace the member so removed.

In the event of a “Motion of no-confidence” governance action to remove all members of the Constitutional Committee at the same time, that is approved by a requisite percentage as specified by the Guardrails of DReps and SPOs, upon implementation of the governance action, the Constitutional Committee shall be considered to be a state of no-confidence until such time as an election has been held either to reinstate the existing Constitutional Committee members in whole or in part, or to elect new Constitutional Committee members.

Section 6

Constitutional Committee processes shall be transparent. The Constitutional Committee shall publish each decision. When voting that a governance action proposed to be executed on-chain is unconstitutional, the Constitutional Committee collectively, or each member of the

Constitutional Committee casting such a vote separately, shall set forth the basis for its decision with reference to specific Articles of this Constitution or provisions of the Cardano Blockchain Guardrails Appendix that are in conflict with a given proposal. Internal deliberation among members of the Constitutional Committee, prior to casting votes, are not required to be publicly disclosed.

The Constitutional Committee shall operate pursuant to a code of conduct periodically adopted and published by the Constitutional Committee. The Constitutional Committee is encouraged to include ethical guidelines in its code of conduct. The Constitutional Committee shall periodically adopt and publish such policies and procedures as the Constitutional Committee shall deem necessary in carrying out its duties.

Section 7

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 8

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 ecosystem may 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. Cardano Blockchain ecosystem budgets shall provide for periodic administrative costs of the Constitutional Committee in such amounts as requested from time to time by the Constitutional Committee and as approved by ada owners.

Section 9

Constitutional Committee members who are also acting as DReps, as SPOs, or both, shall publicly disclose that they are participating in on-chain governance actions in more than one such capacity prior to voting with respect to on-chain governance actions.

ARTICLE VIII. AMENDMENT PROCESS

Section 1

This Constitution should be treated as a living document. Technical advancements, changes in the desires, needs and expectations of the Cardano Community, and unforeseen circumstances may give rise to the need in the future to amend this Constitution. The Cardano Community is encouraged to periodically review and debate its provisions, and when so desired, come together in such forums as the Cardano Community may deem appropriate, to propose amendments to this Constitution. Amendments may be made as provided in this Article VIII.

Section 2

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 satisfying a threshold of not less than 65% of the then active voting stake.

Section 3

If the Cardano Blockchain Guardrails Appendix sets forth an amendment threshold for a Guardrail that is different than the amendment threshold contained in Section 2 of this Article VIII, then the threshold set forth in the Cardano Blockchain Guardrails Appendix for such Guardrail shall apply.

APPENDIX I: CARDANO BLOCKCHAIN GUARDRAILS

1. INTRODUCTION

To implement Cardano Blockchain on-chain governance, 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, functionality or long-term sustainability. As described below, some of these Guardrails are automatable and will be enforced via an on-chain Guardrails Script or built-in ledger rules.

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

Amending, Adding or Deprecating Guardrails

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 anyGuardrails shall require and be deemed to be an amendment to the Constitution itself, including any new Guardrails. Each Guardrail has a unique label. If the text of a Guardrail is amended, the existing Guardrail will be deprecated and a new label will be used in this Appendix. Similarly, if a Guardrail is completely deprecated, its label will never be reused in the future. In all cases, the Guardrails that apply to a governance action will be those in force at the time that the governance action is submitted on chain, regardless of any later amendments.

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” or "must not" be set below or above some value, this means that theGuardrail 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 Blockchain 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, 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, 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, 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 but 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 Guardrails 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 Cardano Blockchain from ever enacting a Hard Fork action, resulting in deadlock. There are three different situations that apply to Guardrail Script usage.

Symbol and Explanation

- (y) The Guardrail Script can be used to enforce the Guardrail.
- (x) The Guardrail Script cannot be used to enforce the Guardrail.
- (~ - reason) The Guardrail 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 Guardrail Script **must not** permits any changes to the parameter.

Conversely, where a parameter is explicitly listed in this document but no checkable Guardrails are specified, the Guardrail Script **must not** imposes 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, to avoid ambiguity, this Appendix uses the parameter name that is used in protocol parameter update governance actions rather than any other 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-02a (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-03a (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-04a (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 registrationlovelace 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* (*committeeMaxTermLength*)

GUARDRAILS

PARAM-05a (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-06a (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;
2. Ensure that stake pools are adequately rewarded for maintaining the

Cardano Blockchain;
3. Ensure that ada owners 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 owners, 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, 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, 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 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
- Provides protection against low-cost denial of service attack on UTxO storage. 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.

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

i) The acceptable cost of attack

ii) The acceptable time for an attack
iii) The acceptable memory configuration for full node users
iv) The sizes of UTxOs 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 the Cardano Blockchain

- 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. Cardano 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-03a (x - "exceptional circumstances") *maxBlockBodySize* **must not** be decreased, other than in exceptional circumstances where there are potential problems with security, performance, 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-04a (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-04a (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.

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 Blockchain network in terms of decentralization and protection against adversarial actions
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. Cardano 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 stake pools when the network is in the equilibrium state

- Primarily a security parameter, ensuring decentralization by stake 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

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. Cost models are defined for each Plutus language version. A new language version may introduce additional cost model values or remove existing cost model values.

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-03a (~ - 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

Triggers for Change

Changes to governance parameters may be triggered by:

1. Cardano 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 (committeeMaxTermLength)

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

GUARDRAILS

CMTL-01a (y) *committeeMaxTermLength* **must not** be zero

CMTL-02a (y) *committeeMaxTermLength* **must not** be negative

CMTL-03a (y) *committeeMaxTermLength* **must not** be lower than 18 epochs (90 days, or approximately 3 months)

CMTL-04a (y) *committeeMaxTermLength* **must not** exceed 293 epochs (approximately 4 years)

CMTL-05a (x - "should") *committeeMaxTermLength* **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, 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-01a (x) 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

TREASURY-02 (x) Withdrawals from the Cardano Blockchain treasury made pursuant to an approved Cardano Blockchain ecosystem for the Cardano Treasury **must not** exceed the net change limit for the Cardano Treasury's balance per period of time

TREASURY-03 (x) Withdrawals from the Cardano Blockchain treasury **must** be denominated in ada

TREASURY-04a (x) Withdrawals from the Cardano Blockchain treasury **must not** be ratified until there is a Cardano Community approved Cardano Blockchain ecosystem 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-02a (~ - no access to existing parameter values) 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-04a (x) At least 85% of stake pools by active stake **should** have upgraded to a Cardano Blockchain 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-01a (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 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-01a (x) A **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. LIST OF PROTOCOL PARAMETER GROUPS

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

The network parameter 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 parameter 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 parameter 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 parameter group consists of:

- *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* (*committeeMaxTermLength*)

APPENDIX II: FRAMING NOTES AND DEFINITIONS

These Framing Notes and Definitions are intended to provide guidance in interpreting this Constitution. The Constitutional Committee should consider this Appendix II as it deems relevant and useful in carrying out its constitutional duties.

FRAMING NOTES

The Cardano Blockchain was established in 2017. In July 2020 the Cardano Blockchain was expanded to include independent block validators and in September 2024 an on-chain governance system was introduced. This Constitution outlines the rights and responsibilities of governance actors in the decentralized system who represent the owners of ada, the governance token of the Cardano Blockchain. The Cardano Blockchain is presently a decentralized ecosystem of blockchain technology, smart contracts, and community governance.

In approaching this Constitution, the Cardano Community recognizes that 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 participants in the Cardano Community 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.

DEFINITIONS

	active block production stake	Means, in relation to SPOs, the number of lovelace which is actively delegated to the SPO for the purpose of block production.

	active voting stake	Means the total number of lovelace which is considered active, based upon required voting activity and registration to vote, as specified in the Guardrails and counted for the purposes of determining a vote.
	ada	Means the cryptocurrency which is native to the Cardano Blockchain
	ada owner	Means the person or entity that has legal title to ada as determined by applicable law.
	Cardano Blockchain	Means the public, proof-of-stake, peer-to-peer, distributed ledger system operating under the name "Cardano."
	Cardano Blockchain ecosystem	Collectively refers to the interconnected and interdependent network of participants in the Cardano Community who have or may come together to support, develop, advance and maintain the Cardano Blockchain pursuant to shared principles and a common vision as enshrined by the Constitution.
	Cardano Blockchain ecosystem budget	Means, for any given period, the allocation of ada from the Cardano Blockchain treasury that has been approved in accordance with the Constitution in order to fulfill the permitted uses of the Cardano Blockchain treasury set forth in Article IV.
	Cardano Community	All owners of ada, all developers of, all those building on, and all those otherwise supporting, maintaining, contributing to, or using the Cardano Blockchain, whether individuals or organizations, are deemed to collectively constitute the Cardano Community.
	Cardano Blockchain treasury	Means the decentralized on-chain ada management system that holds and releases ada received from transaction fees and monetary expansion.
	Constitutional Committee or CC	Means the governing body responsible for determining that governance actions implemented on-chain are constitutional.

	delegator	Means an ada owner who delegates its voting stake to one or more DReps in order to vote with respect to on-chain governance actions.
	Delegated Representative or DRep	Means an individual or entity who has registered to vote with respect to on-chain governance actions for its own behalf or on behalf of other owners of ada.
	epoch	Means a fixed time period of time to provide all SPOs a common frame of reference for scheduled events on the Cardano Blockchain.
	expected	As used in this Constitution, “expected” is intended to represent a reasonable presumption that the identified action, although not mandatory, will occur.
	governance action	Means an action to record information on, take action in relation to, or modify the parameters of, the Cardano Blockchain which has been submitted for an on-chain vote.
	Guardrail	Means the conditions and parameters set forth in the Cardano Blockchain Guardrails Appendix required to maintain the functionality, security and performance of the Cardano Blockchain, some of which, but not all, are directly implemented on the Cardano Blockchain.
	Guardrails Script	Means the plutus script that is recorded on-chain and that enforces the automatable Guardrails when a Governance Action is implemented on-chain.
	lovelace	Means a unit of ada, with one million lovelace to every one ada.
	net change limit	Means the limit in ada by which the Cardano treasury shall not change in a given period.
	on-chain and off-chain	"on-chain" refers to governance actions which are implemented or otherwise recorded on the Cardano Blockchain, and "off-chain" refers to proposed governance

		actions which have not yet been implemented or otherwise recorded on the Cardano Blockchain or other types of governance related decisions that are not intended to be implemented or otherwise recorded on the Cardano Blockchain.
	parameters	Means settings and limits for the implementation of the Cardano Blockchain which are specified in the Constitution.
	predefined auto abstain voting option	Means a delegation of an ada owner's voting stake to an ongoing vote of abstain.
	protocol	Means the algorithms, rules and procedures governing the operation of the Cardano Blockchain
	Stake Pool Operator or SPO	Means each person or entity running a Cardano block-producing node.