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 and the rights of ada owners.

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 for as long as they wish, while honoring the freedom to take another path.

DEFINED TERMS

1. Active Voting Stake. The total amount of lovelace that is delegated to active DReps or SPOs. This stake is used as the basis for calculating voting thresholds and adjudicating proposed Governance action outcomes. It excludes stake delegated to inactive DReps, the predefined abstain voting option, unregistered stake, and registered undelegated stake.

2. Cardano Community. The collective group of all individuals and organizations that, in embracing the shared principles and objectives set forth in the Cardano Blockchain Ecosystem Constitution, own ada, develop, build on, support, maintain, contribute to, and use the Cardano Blockchain.

3. Cardano Community Member. Any participant, individual or organization in the Cardano Community, including the CC.

4. Constitutional Committee (CC). The governing body and its component elected seats charged with ensuring that applicable governance actions take effect on the Cardano Blockchain only if in alignment with the principles and provisions set forth in the Cardano Blockchain Ecosystem Constitution.

5. Constitutional Committee member (CC member). A person, whether an individual or organization, that serves as a member of the Constitutional Committee.

6. Delegated Representative (DRep). The individual or entity registered to vote with respect to on-chain governance actions on its own behalf or on behalf of other ada owners.
7. Net Change Limit. The maximum allowed amount or percentage of lovelace that may be removed from the Cardano Treasury in a given period.
8. Stake Pool Operator (SPO). An individual or entity that controls cold key(s) of a block-producing node of a Stake Pool.
9. Stake Pool. A Stake Pool Operator's block producing node, identified by a unique Stake Pool ID, which aggregates applicable Delegator stake, forges and validates Blocks, and facilitates contributions of the SPO to the Cardano Blockchain's security, decentralization, consensus mechanism, and governance process.
10. Treasury Withdrawal Recipient. A person or entity who is indicated as the recipient of ada from the Cardano Treasury in the relevant "Treasury Withdrawals" action.

ARTICLE I. CARDANO BLOCKCHAIN TENETS AND GUARDRAILS

Section 1 Guiding Tenets

The following Tenets shall guide all Cardano Community members and proposed governance actions shall be evaluated in accordance with these Tenets. The order in which the Tenets below 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 be unreasonably 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 ada 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 fairly and impartially, taking into account the collective desires of the Cardano Community, consistent with the long-term sustainability and viability of the Cardano Blockchain.

TENET 10 The Cardano Blockchain's monetary system shall promote financial stability. This shall include seeking to preserve the value and utility of ada as a medium of exchange, store of value, and unit of account. The total supply of ada shall not exceed 45,000,000,000 (45,000,000,000,000,000 lovelace).

Section 2 Implementation of Guardrails

1. The Cardano Blockchain shall operate in accordance with the Cardano Blockchain Guardrails Appendix to this Constitution. The Cardano Community may digitally codify certain Guardrails such that the Guardrails are directly programmed and implemented on the Cardano Blockchain using on-chain Guardrails Script or built-in ledger rules.

2. 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. The CC shall seek to reconcile such inconsistencies through the encouragement of an appropriate on-chain governance action.

ARTICLE II. COMMUNITY AND GOVERNANCE

Section 1 The Cardano Community

1. No formal membership shall be required to use, participate in and benefit from the Cardano Blockchain. Cardano Community members are entitled to the rights, privileges, and protections of this Constitution, and are accordingly expected to support and uphold this Constitution, maintain the integrity of the ecosystem, participate in governance, and resolve disputes transparently.

2. Cardano Community members are encouraged to collaborate on developing applications and to form organizations that support the Cardano Blockchain and the Cardano Community.

Section 2 Participation Rights of ada owners

1. Ada owners are entitled to access and participate in the on-chain decision-making processes of the Cardano Blockchain ecosystem, including voting, proposing changes to the governance structure in accordance with the Guardrails, and otherwise taking part in on-chain governance actions.

2. Ada owners can directly participate in governance actions by registering as DReps themselves or by delegating their voting rights to other registered DReps.

3. Any ada owner shall be allowed to register as a DRep. A DRep may act in the interest of one or more ada owners.

4. Any ada owner shall be allowed to delegate their voting stake to one or more registered DReps, including themselves.

5. Ada owners shall be allowed to change the delegation of their voting stake at any time.

6. Ada owners 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, and to delegate the voting rights of the ada owner to registered DReps on the owner's behalf.

7. Ada owners have the right to a process for participating in, submitting and voting on on-chain governance actions that is open, transparent, and protected from undue influence and manipulation.

Section 3 Decentralized Governance Framework

1. The Cardano Blockchain is governed by a decentralized, on-chain model that, where beneficial, uses smart contracts and other blockchain tools to facilitate decision-making and ensure transparency.

2. Three independent voting bodies - DReps, SPOs, and the CC - participate in on-chain voting; anyone holding multiple roles must publicly disclose such overlaps before engaging in any on-chain governance actions.

Section 4 Delegated Representatives

1. DReps have voting power equal to the number of lovelace delegated to them.

2. DReps may vote on all types of governance actions.

3. DReps shall ensure that any compensation received in connection with their activities as a DRep is publicly disclosed in a timely manner through relevant governance communication channels.

4. DReps shall not offer or provide compensation to an ada owner in exchange for being appointed as a DRep or for voting on their behalf.

Section 5 Stake Pool Operators

1. SPOs shall vote on the following governance actions: "No Confidence", "Update Committee", "Hard Fork Initiation", "Parameter Update" that affect security-relevant parameters, and "Info" actions.

Section 6 Governance Action Standards

1. To ensure transparency in on-chain governance, proposed governance actions shall follow a standardized and legible format before being recorded or enacted on-chain. This format shall include a URL hosting a document that outlines additional context for the proposed governance action, and the hash of this document. The document hosted by such a URL shall be immutable and incapable of being altered after submission, and the content of every on-chain Governance Action must be identical to the final off-chain version of the proposed action.

2. Each proposal shall provide sufficient rationale, including at minimum: a title, abstract, justification, and relevant supporting materials.

3. "Hard Fork Initiation" and "Parameter Update" 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.

Section 7 "Treasury Withdrawals" Action Standards

A "Treasury Withdrawals" action must, in addition to the requirements at Section 6, meet all of the following requirements:

1. "Treasury Withdrawals" actions must specify the terms of the withdrawal. This shall include: the purpose of the withdrawal, the period for delivery of proposed activities which the withdrawal shall be used for, the relevant costs and expenses of the proposed activities, circumstances under which the withdrawal might be refunded to the Cardano Treasury.
2. "Treasury Withdrawals" actions shall disclose whether the prospective recipient of the "Treasury Withdrawals" action has received ada from the Cardano Treasury within the last 24 months.
3. A Net Change Limit must be set. "Treasury Withdrawals" actions must not exceed the Net Change Limit for that period.
4. "Treasury Withdrawals" actions 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.
5. "Treasury Withdrawals" actions shall designate one or more administrators responsible for monitoring how the funds are used, and ensuring the deliverables are achieved.
6. Any ada received from a Cardano Blockchain treasury withdrawal, so long as such ada is being held by an administrator prior to further disbursement to the Treasury Withdrawal Recipient, must be kept in one or more separate accounts that can be audited by the Cardano Community, and such accounts shall not be delegated to an SPO but must be delegated to the predefined abstain voting option.

ARTICLE III. CONSTITUTIONAL COMMITTEE

Section 1 Role and Scope

1. A CC 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.
2. Each CC member shall have one vote.
3. No governance action - other than a "No Confidence" or "Update Committee" action - may be implemented on-chain without affirmation by a requisite percentage of CC members.
4. The CC shall be limited to voting on the constitutionality of governance actions, including any proposed or contemplated actions contained within "Info" actions.

Section 2 Composition and Terms

1. The CC shall be composed of such number of members and serve such term lengths as are sufficient to assure the ongoing integrity of the Cardano Blockchain, as determined from time to time by Ada owners.

2. To assure continuity in the operation of the CC, the terms for CC members shall be staggered.

Section 3 Election Process, No Confidence and Removal

1. The CC 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 CC must be reinstated or replaced using the "Update Committee" action before any other on-chain governance action, other than "Info" actions, may go forward.
2. The Cardano Community shall establish and make public a process from time to time for election of members of the CC consistent with the requirements of the Guardrails.
3. In the event of a vote of no confidence or the removal of some CC members by "Update Committee" action, an election shall be held as soon as practical.

Section 4 Transparency and Conduct

1. CC processes shall be transparent, and the CC shall publish each decision.
2. When voting that a governance action proposed to be executed on-chain is unconstitutional, each CC member casting such a vote 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.
3. CC members may be compensated for their efforts as members and shall ensure that any compensation received in connection with such activities is disclosed in a timely manner through relevant governance communication channels.

ARTICLE IV. AMENDMENT PROCESS

Section 1 Amendment Rules

Amendments to this Constitution, including the Cardano Blockchain Guardrails Appendix, shall require approval via an on-chain governance action supported by at least 65% of the active voting stake at that time, unless a different threshold is expressly provided in the Cardano Blockchain Guardrails Appendix for the amendment of a particular Guardrail, in which case that threshold 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, research, measurement, and governance objectives.

These Guardrails are designed to avoid both unexpected and foreseeable 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 tightened in due course.

Additional Guardrails may also be needed where, for example, new protocol parameters are introduced or existing ones are removed.

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 any Guardrails 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 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

This section provides supplementary definitions and interpretive guidance for terms used throughout this Constitution and the Guardrails Appendix.

Cardano Blockchain. The decentralized, public, peer-to-peer, proof-of-stake distributed ledger system, designed to securely record, verify, and synchronize transactions and data across the network while enabling the execution of smart contracts and decentralized applications. This system, powered by ada, is the longest chain of blocks with sufficient confirmations to be considered finalized starting from block Hash 5f20df933584822601f9e3f8c024eb5eb252fe8cefb24d1317dc3d432e940ebb, as forged on 2017-09-23 21:44:51 UTC on the Cardano Network.

Block. A container of data produced by a Stake Pool that includes, at minimum, a header. Block production and block forging are used interchangeably.

Protocol. The algorithms, rules, and procedures that govern the exchange of information on the Cardano Blockchain.

Protocol Parameters. Protocol settings that define how the Cardano Blockchain functions; modifiable through applicable governance processes.

Slot. The smallest denomination of time nested within an Epoch.

Epoch. A Protocol-determined interval characterized by a fixed number of Slots. Each Slot's duration and sequence are governed by the blockchain's consensus mechanisms and are associated with a universal timestamp defined in UTC. It is used for operations including governance voting, Block production leadership determination, rewards calculation, and Hard Forks.

lovelace. The smallest unit of value for the native cryptocurrency of the Cardano Blockchain, utilized for the network's security and governance. It is distinguished from other native tokens by its lack of a policy ID and policy name.

ada. A superunit of lovelace, with 1 ada equal to 1,000,000 lovelace.

Delegator. A private key holder that delegates stake to a Stake Pool for block production and network security, to a DRep for participation in on-chain governance, or both. In doing so, the delegator contributes to the operation and governance of the Cardano Blockchain.

Active Block Production Stake. The cumulative amount of stake, measured in lovelace, that is actively delegated to Stake Pools and utilized for block forging during the current Epoch. This amount is determined by a snapshot of stake distribution taken at the beginning of the previous Epoch, ensuring that it accurately represents the effective stake available for securing and maintaining the Cardano Blockchain through block forging.

On-chain. A classification for actions, transactions, or governance activities that are executed, recorded, or implemented directly on the Cardano Blockchain. These actions, transactions, or governance activities are permanently validated and stored through the blockchain's consensus mechanism, ensuring their immutability and transparency.

Off-Chain. A classification for activities, proposals, or governance decisions that are either not yet implemented on the Cardano Blockchain, or not intended to be directly recorded on the blockchain. These may include discussions, proposals, or agreements that exist outside the blockchain and do not involve direct consensus or on-chain validation.

Governance Action. An on-chain proposal enabling participation in shaping the future of the Cardano Blockchain Ecosystem through voting transactions.

Hard Fork. A Protocol upgrade for the Cardano Blockchain that results in a new Protocol version and necessitates coordinated adoption by network participants.

Guardrails. A set of restrictions on Governance Actions to prevent undesirable outcomes and assist voters in deciding whether the proposed action complies with the Cardano Blockchain Ecosystem Constitution. Some guardrails are enforced using the Guardrails Script or ledger rules to prevent submission of the action, while others necessitate further adjudication to determine if they violate the Constitution in ways the Guardrails Script or ledger cannot check. Guardrails may be either mandatory

("must"/"must not") or advisory ("should"/"should not"). The latter allows for interpretive flexibility where necessary.

Guardrails Script. A smart contract script that checks specific proposed Governance Actions, "Hard Fork Initiation" and "Parameter Update" actions, against automatically checkable Guardrails. The check is applied when the Governance Action is proposed on-chain.

Motion of no confidence governance action ("No Confidence" action). A motion to create a state of no confidence in the current constitutional committee.

Update committee and/or threshold and/or terms governance action ("Update Committee" action). Changes to the members of the Constitutional Committee and/or to its signature threshold and/or terms.

New Constitution or Guardrails Script governance action ("New Constitution" action). A modification to the Constitution or Guardrails Script, recorded as on-chain hashes.

Hard Fork Initiation governance action ("Hard Fork Initiation" action). Triggers a non-backwards compatible upgrade of the network; requires a prior software upgrade.

Protocol Parameter Changes governance action ("Parameter Changes" action or "Parameter Update" action). Any change to one or more updatable protocol parameters, excluding changes to major protocol versions ("hard forks").

Treasury Withdrawals governance action ("Treasury Withdrawals" action). Withdrawals from the treasury.

Info action ("Info" action). An action that has no effect on-chain, other than an on-chain record.

Cardano Blockchain Treasury, Cardano Treasury, or Treasury. A supply of ada controlled by the Protocol of the Cardano Blockchain; collected from transaction fees, reserves, and other designated sources. Withdrawals from this supply of ada are subject to the processes and restrictions set forth in the Cardano Blockchain Ecosystem Constitution.

Cardano Blockchain Ecosystem. The collective ecosystem comprising the Cardano Blockchain, the Cardano Community, and the tooling and infrastructure utilized by the Cardano Community to support the Cardano Blockchain in alignment with the shared principles and objectives set forth in the Cardano Blockchain Ecosystem Constitution.

Expected. A reasonable presumption that the identified action, although not mandatory, will occur.

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 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 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 sustainability of the Cardano Blockchain network
- Severity 2 is a major incident or issue with significant impact to the security, performance, functionality or sustainability of the Cardano Blockchain network
- Severity 3 is a minor incident or issue with low impact to the security, performance, functionality or 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 Withdrawals" action.

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 permit 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 impose any constraints on changes to the parameter.

2. Guardrails and Guidelines on "Parameter Update" actions

Below are Guardrails and guidelines for changing updatable protocol parameter settings via the "Parameter Update" 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 "Parameter Update" 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" 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) A parameter that is critical to the operation of the blockchain requires 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 90 days should normally pass between the publication of an off-chain proposal to change a parameter that is critical to the operation of the blockchain 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* (*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 90 days 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:

$fee(tx) = txFeeFixed + txFeePerByte \times nBytes(tx)$

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 *txFeePerByte* should be adjusted whenever Plutus Execution prices are adjusted (executionUnitPrices[steps/memory])

TFGEN-02 (x - "unquantifiable") Any changes to *txFeeFixed* or *txFeePerByte* 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

1. The acceptable cost of attack
2. The acceptable time for an attack
3. The acceptable memory configuration for full node users
4. The sizes of UTxOs and
5. 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

1. the cost of executing a transaction with maximum CPU steps is similar to the cost of a maximum sized non-script transaction and
2. 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 effect - economic advice based on analysis 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 based on analysis 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 units

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-03a (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 (65 days)

DRA-02 (y) *dRepActivity* must not exceed 37 epochs (185 days)

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 (60 days, 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-02a (y) Economic, network and technical/security 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 Initiation" action thresholds must be in the range 51%-80%

VT-CON-01 (y) "New Constitution" action thresholds must be in the range 65%-90%

VT-CC-01 (y) "Update 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 (e.g., 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 "Parameter Update" 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 Withdrawals" Actions

"Treasury Withdrawals" 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-02a (x) Withdrawals from the Cardano Blockchain treasury must not exceed the Net Change Limit for the Cardano Treasury's balance per period of time

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

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 Committee" actions

"Update Committee" actions may change the size, composition or required voting thresholds for the Constitutional Committee.

GUARDRAILS

UPDATE-CC-01a (x) "Update Committee" actions must not be ratified until ada owners have ratified through an on-chain governance action this Constitution

6. Guardrails and Guidelines on "New Constitution" actions

"New Constitution" 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/security 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* (*govDeposit*)
- *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. SUPPORTING GUIDANCE

This Appendix II is intended to provide guidance in interpreting the Constitution and the Constitutional Committee shall consider this Appendix II as it deems relevant and useful in carrying out its constitutional duties.

1. 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 ada owners; ada is the governance token of the Cardano Blockchain. The Cardano Blockchain is a decentralized ecosystem of blockchain technology, smart contracts, and community governance.

In approaching this Constitution, the Cardano Community recognizes that this is not a constitution for only a blockchain but rather a constitution for a blockchain ecosystem. 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 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 - including ada owners acting directly as 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 Blockchain treasury through the inclusion of the Cardano Blockchain Guardrails in this Constitution.

2. Other Guidance

The drafters of the Constitution, together with other participants from the Cardano Community, have published and in the future may publish guidance for interpreting the Constitution, including, without limitation, a definition booklet that has been released contemporaneously with the on-chain ratification of the Constitution. So long

as any such published guidance has been hashed to the Cardano Blockchain pursuant to an "Info" action, the Constitutional Committee shall not be precluded from considering and utilizing such guidance as it deems appropriate.