Designing Policy for a Flourishing Blockchain Industry

Decentralization Research Center

April 2025 Edition

About Decentralization Research Center

The Decentralization Research Center (DRC) is a 501(c)(4) social welfare non-profit that advocates for decentralization as a fundamental characteristic of emerging technologies. This includes the development of blockchain protocols and applications that are immutable, censorship resistant, transparent, secure, and enable data self-sovereignty.

Authors: Sarah Brennan and Connor Spelliscy

Thanks to members of Filecoin, Chia, Aave, Dragonfly, Uniswap, Institute of Free Technology, Ethereum Enterprise Alliance, Etherealize, Ethereum Naming Service, Digital Currency Group, Eigen Layer, DeFi Education Fund, MetaLex Labs, Electric Coin Co., Delphi Ventures, a16z Crypto, 1kx, Predicate, ZKsync, Optimism, Lido, and other teams/communities for discussions and feedback that informed the updates in this draft. Views expressed in this paper do not necessarily reflect the views of those who provided feedback.

Cover photo: Artem Krapivin

Table of Contents

Introduction

Introduction to the Revised Edition

This updated edition of *Designing Policy for a Flourishing Blockchain Industry* reflects over a month of dialogue, collaboration, and feedback from a wide range of organizations, researchers, developers, policy advocates, and policymakers. It includes structural refinements and clarifications to our original decentralization framework, along with a reframing that better aligns with how the principles are likely to be implemented across the policy landscape. The revisions reaffirm core values of the crypto ecosystem while preserving the flexibility needed to foster innovation and adapt to ongoing change.

Foundational Values Behind the Decentralization Principles

It is important to note that the decentralization principles in this report are not new constructs. They are a deliberate implementation of long-standing principles advanced by the cypherpunk and open-source communities — values that have shaped the blockchain ecosystem from its inception. As recently articulated here, these include: open participation, distributed control for system resilience, censorship resistance, auditability, credible neutrality, and a focus on collaborative tool building over empire building. These values are fundamentally about building trustless systems that empower users without reliance on coercive authority.

However, these values are not easy to uphold. Many systems today that claim to be decentralized fall short, as the ease of adopting centralized shortcuts has prevailed in the absence of regulatory incentives. Falling prey to the temptation of centralization or worse, legislatively incentivizing centralization and reintermediation, puts us in danger of recreating existing systems but with extra costs and inefficiencies.

The result — blockchain implementations of legacy systems — poses a net negative for society, introducing additional security risks, novel systemic risks, and, remarkably, becoming more extractive than the very systems they aim to replace.

This makes it all the more urgent to design regulatory frameworks that actively incentivize these values rather than reward their erosion. As such, the goal of this effort is to translate these values into administrable legal criteria and advocate for their inclusion in policy that shapes the future of public infrastructure.

The Task Ahead on Blockchain Policy

Blockchain technology can provide users with unprecedented levels of transparency, reliability, and security — as long as policy frameworks allow it to flourish.

If properly regulated, blockchain technology facilitates decentralization, giving users greater control over their finances and digital assets, reducing reliance on overreaching institutions. Beyond financial use cases, decentralized blockchain networks function as infrastructure for a variety of applications that provide users with more autonomy over their lives, including, for example: social media platforms that allow users to own and control their data, community-owned platforms that leverage decentralized governance to compete with Big Tech, and digital identity protocols necessary for users to protect their identity online from sophisticated AI-enabled bots.

Blockchain technology can provide users with unprecedented levels of transparency, reliability, and security — as long as policy frameworks allow it to flourish.

The policy decisions made in the next two years will shape the trajectory of this technology for decades to come. If policy conflates decentralized and centralized blockchain technology, it will remove the incentives needed for decentralization — an inherently more complex and resource-intensive path — making centralization the default and negating the benefits and risk mitigation that blockchains enable. Without clear regulatory distinctions, builders will have strong incentives to develop centralized blockchains, as they are cheaper to run, easier to control, and allow the founders to build a walled garden to capture and extract value from users. These systems offer little meaningful improvement over legacy systems, continuing the cycle of gatekeeping and limiting user autonomy rather than fostering the open, permissionless innovation that decentralization enables.

The best-case scenario for blockchain policy is one that enables a flourishing ecosystem of digital infrastructure, applications, and businesses that provide significant autonomy and economic opportunity to users. The worst-case scenario is a policy framework

that fails to incentivize decentralization and innovation, instead creating loopholes that enable opportunists to bypass securities laws and exploit retail investors.

Defining Decentralization Under Law

A key challenge for policymakers is that there is no universally accepted definition for a decentralized blockchain or digital asset. However, over the past several years, academic research and industry experience have helped us to better understand how to implement a decentralization test under law, including where to draw the lines at the legislative and regulatory levels.

Based on our review of relevant literature and work in the industry, we believe that focusing on control is the most effective framing option for defining decentralization under law. SEC Commissioner Peirce referenced control in the context of blockchain decentralization in her 2019 Framework, and articulated it in more detail in a 2020 speech. Meeting a test for control would significantly reduce information asymmetries stemming from the control of a blockchain's token, justifying lower regulatory burdens or exemptions under securities laws. Further, based on our many conversations with industry stakeholders, there is a strong and growing consensus that anchoring legislative and regulatory tests to points of control provides a cohesive, coherent, and actionable means of aligning regulatory incentives to build trustless systems while allowing regulators to address risks posed by retained points of control.

We believe that focusing on control is the most effective framing option for defining decentralization under law.

From an implementation standpoint, it is essential to align the control principles with the specific regulatory context. At the legislative level, these principles should be expressed at a high level, while granting implementing agencies the authority to issue detailed guidance and establish rules-based exemptions. This includes the use of safe harbors and other regulatory mechanisms designed to provide targeted and comprehensive relief consistent with the overarching principles.

The first implementation of the principles could be featured in a forthcoming token classification framework, whether through market structure legislation currently being developed in Congress or through an SEC-issued safe harbor. Both approaches aim to address the securities status of tokens and determine how they may be legally

traded. Notably, a decentralization test was included in H.R. 4763, the Financial Innovation and Technology for the 21st Century Act. While that version of the test marked an important and commendable step forward, which informed some of our work below, it followed a rules-based approach with several distinct criteria that were not clearly unified under a principle like "control." This structure, while a great start, made the test comparatively challenging to apply consistently across a broad range of projects.

We believe Congress should instead ground the decentralization test in the principle of "control" by adopting a hybrid approach: a principles-based framework supplemented by rules-based safe harbors and other exemptive relief. At the SEC level, we have already recommend the introduction of two safe harbors: Rule 195, which would provide prospective regulatory clarity for new token distributions, and Rule 195T, which would offer transitional and retroactive relief for past issuances. We outlined these proposed safe harbors in detail in our recent submission to the SEC.

Below we propose seven principles to be applied in control-based decentralization tests. *Outside of the context of trading tokens, we believe that it is not necessary to weigh these principles equally or even use all of these principles in all cases*, as there should be a path to compliance for all types of blockchain projects. However, these principles would be particularly relevant when considering the securities treatment of layer-one blockchains, which provide foundational infrastructure upon which applications and businesses are built.

The principles are technology-neutral across distributed ledger technologies and are evergreen, meaning any current or future blockchain network can meet the standard. The principles were designed such that verification would rely primarily on the network's source code, with additional transparency provided through mandatory disclosures when necessary.

Carveouts to the principles should also be implemented to balance competing policy interests, such as user safety. For instance, where a security council retains narrowly constructed special powers in case of incident. These sorts of exceptions should be limited and apply only when necessary.

Control Principles for Decentralization

In this revised version, we have included a simple articulation of each principle, the policy rationale for its inclusion, an example implementation, and a section that summarizes key considerations and potential carveouts identified through continued dialogue with industry stakeholders.

1. Open Blockchain Network

Principle: Source code is publicly available and open source.

Infrastructure must operate in a way that is provably fair to all participants, such that anyone can verify that the system does not embed favoritism or hidden influence. Moreover, open networks rely on network effects to operate effectively, with the token serving as the primary value accrual mechanism that incentivizes broad and sustained participation.

Open source requirements are an essential factor in establishing a standard for reducing control.

The principles for Open Blockchain Networks were originally proposed in Defining Decentralization for Law in 2020 and have been echoed in subsequent efforts like Regulation X.

Policy Rationale: Closed software systems can subject their users to a number of risks, given that the source code is not made available to users to audit. Securitizing ownership of such software should remain subject to securities laws.

These risks can be reduced through open blockchain networks that make their source code freely and publicly available so third parties can audit the code. Open source requirements are an essential factor in establishing a standard for reducing control and providing users with the ability to verify how a protocol functions. Many open-source licenses also enable participants to fork the underlying blockchain, which, while not a panacea due to the practical implementation issues, offers an escape hatch if a critical mass of users choose to exit to run their own version of a protocol.

Example Implementation:

> *The blockchain network is either: (a) a blockchain whose source code is freely and publicly available open-source code; or (b) a blockchain protocol whose source code is freely and publicly available open-source code and is recorded for execution by clients on a blockchain of the kind described in clause (a).*

Discussion of Limits and Potential Carveouts: Industry stakeholders held positions ranging from advocates for full transparency to those who desired a materiality standard and some lenience for ancillary functions. There are a number of gates market actors use to increase their moats, the lowest hurdle is trademark protection, which is used broadly in the industry. We also frequently discussed carveouts that would assist in defending users against phishing attacks.

Stronger forms of IP protection and proprietary models, particularly at the application layer, are increasingly used to establish competitive moats. These range from source-available or BSL (Business Source License) models to fully proprietary implementations, where the code is non-public and its operation is a black box. We believe this trend risks a slippery slope back toward a proprietary Web 2.0 paradigm, especially if regulation is too permissive. However, the specific context in which these restrictive IP measures are applied will be crucial in assessing whether such licenses align with the principles. This issue may warrant additional regulatory guidance and rulemaking as agencies implement the broader legislative framework.

2. Autonomous Blockchain Network

Principle: The network operates without intervention using pre-established rules encoded in the source code.

This principle operates as a check on resilience and incentivizes the elimination of single points of control and failure. It does so by ensuring systems are distributed and operate in a trustless environment with smart contracts and mechanisms that enforce rules consistently and predictably. This makes the network more resilient to attacks and outages versus those that rely on, or can be arbitrarily altered by, a

control group. This principle minimizes the risk of systemic failures and, even if parts of a system are compromised, the overall network can remain secure and operational.

Policy Rationale: By operating autonomously, a blockchain network removes the need for a central authority, thereby eliminating single points of control and failure with respect to both the network and its token. For blockchains, if certain nodes or participants go offline or are compromised, the system continues to function because the control is distributed — autonomous functioning reduces the risk of systemic failure or attack. Further, autonomous functioning ensures that the systems operate based on rules that are transparent and enforced through code, meaning that participants can trust the system without the need to trust one another or any central authority. As a result, control-related risks for all participants are substantially reduced.

Meeting this principle also ensures a network is "functional," which is a requirement that was previously included in the Financial Innovation and Technology for the 21st Century Act in 2023, and can be traced back to the SEC's 2019 Framework for Digital Assets criteria, which focused on systems being "fully developed and operational" and that network tokens be usable in line with their "intended functionality."

By operating autonomously, a blockchain network removes the need for a central authority.

Example Implementation:

> *The blockchain network operates, executes, and enforces its operations and transactions, functioning on pre-established, transparent rules encoded directly within the source code of the blockchain network.*

Discussion of Limits and Potential Carveouts: As a point of clarity, this element is not intended to extend beyond the policy rationale for its inclusion. It is intended to ensure the blockchain network operates autonomously in the ordinary course but is not intended to limit the ability for an initial developer team to continue to work on the network or a prohibition on roadmaps with planned upgrades. It also must have practical limits in its application. For instance, the ability to operate without human intervention is not, itself, a prohibition on human intervention if the potential for human intervention is limited to the transparent rules encoded within the source code, transparent rules disclosed to participants, and compliant with the other factors

in this analysis, as well as other practical limitations stemming from other areas of the law like informational reporting obligations.
Almost every organization we spoke with stressed the need for carveouts to protect user safety. For instance, many networks utilize a security council that retains a narrowly constructed set of special powers in case of a critical security incident.

We discussed the need to match the materiality of offchain elements that may exist in a given model with various stakeholders to the risks this element is intended to address. We also discussed the operation and various functions of decentralized governance and the limits of each and every decision being able to be implemented onchain. Many stakeholders feel that carveouts should be made where centralized offchain points of control have been implemented on the basis of decisions made by decentralized governance. We do not feel that decentralized governance can be a cure-all, but regulatory agencies implementing this legislative framework should give guidance as to the appropriateness of potential delegations made by governance to trusted parties (as well as standards for said parties and governance overall).

3. Permissionless Blockchain Network

Principle: No person or group of persons under common control has unilateral authority to restrict use of the network.

This principle tests the design of the network — specifically, whether the technology is public infrastructure or a privatized tech platform. Permissionlessness ensures users are less vulnerable to actions that could compromise their property rights, be value extractive to their participation, or fundamentally alter the rules of the game. It is also a factor that supports the distribution of power required by the 'autonomous' principle, diminishing the reliance on the original developers and allowing control to be further distributed among active participants.

If a user's participation in a blockchain network can be unilaterally restricted, then the user is subject to significant control-related risks

Policy Rationale: If a user's participation in a blockchain network can be unilaterally restricted, then the user is subject to significant control-related risks stemming from the lack of transparency, potential for collusion, and censorship. Any third party with restricting authority could utilize that power indiscriminately against an individual

tokenholder or all tokenholders, to harm their property rights and extract value. If no such control exists, then tokenholders are free to use and participate in the blockchain network as they see fit and may exit the system at any time, thereby insulating against risks of information asymmetries, conflicts of interest, and value extraction. Permissionlessness is critical to achieving meaningful decentralization. By enabling any third party to interact with and build on the system without needing approval, trust dependencies on the original development team are substantially reduced. As the system evolves, those dependencies should continue to decline, helping mitigate risks tied to information asymmetries.

While some projects may launch with permissionless architectures, for many, introducing permissionlessness too early can pose significant security risks. In such cases, it is more prudent to phase in permissionlessness as the system matures. Accordingly, it may be inappropriate to mandate permissionlessness at launch, but reasonable — and arguably necessary — to require it before insiders are permitted to sell.

This principle was proposed in the Financial Innovation and Technology for the 21st Century Act in 2023.

Example Implementation:

> *The blockchain network does not empower any person or group of persons under common control with unilateral authority to restrict or prohibit use of the blockchain network, including, without limitation: (a) deploying software that uses or integrates with the blockchain network; (b) operating any client, node, validator, or other form of computational infrastructure with respect to the blockchain network; or (c) participating in any decentralized governance system. Notwithstanding the foregoing, it will not be deemed a barrier to open use and participation should a Network implement mechanisms to restrict access provided they are non-discriminatory and designed solely to preserve the security and stability of the Network, such as to mitigate spam or malicious activity, provided further that these mechanisms are transparent, equitable, and do not impose unreasonable barriers to participation.*

Discussion of Limits and Potential Carveouts: It has long been understood that certain carveouts would be necessary for this principle, a view consistently echoed in our discussions with stakeholders. As a result, we included a basic carveout to clarify that this principle should not be interpreted as prohibiting consensus mechanisms that enable open but economically rational participation, the use of transaction fees to incentivize network engagement, or user safety measures such as rate limiting.

During discussions with industry it became clear that there should also be carveouts in (c) for the operation of transparent onchain decentralized voting systems which may impose voting standards (i.e., a staking requirement to vote) or other mechanisms to ensure fairness and the alignment of incentives or to discourage gaming and self-dealing.

Questions were also raised about the scope of (b) as it relates to computational infrastructure, particularly given its potential implications for various application-layer technologies and L2 solutions. We believe materiality plays an important role in this analysis. The context in which more restrictive, permissioned elements are applied, both in terms of timing and function, will be critical in assessing whether they align with this principle. These issues may warrant further regulatory guidance and rulemaking during the implementation of the legislative framework.

There are also a variety of mechanisms employed that amount to soft-permissioning that will test the outer limits of this element, whereby regulators will likely be tasked with providing guidance as to whether the spirit of this principle is met.

4. Non-Custodial Blockchain Network

Principle: Participants can maintain total independent control of their digital assets, governed solely by their private keys.

Policy Rationale: Total independent control is a longstanding concept in regulations relating primarily to money transmission. For example, the FinCEN 2019 guidance includes a "total independent control" test with respect to multiple signature wallet providers, but the test is also applicable on a broader basis for assessing non-custodial networks

for purposes of market structure regulation. With respect to a non-custodial network, the factors should be: (a) the value belongs to the owner; (b) the owner interacts with software or other technology to initiate a transaction, supplying the necessary credentials required to access the value; and (c) any other person or group that provides software tools, additional validation, or other non-essential services in a transaction at the request of the user never has total independent control over the value.

Non-custodial technologies ensure that only the user has the authority to make decisions or take actions, such as transferring or moving their crypto assets. This principle is supported by existing guidance and is codified in 31 CFR § 1010.100(ff), which clarifies that providers of "delivery, communication, or network access services" used to support a user's activity are not financial intermediaries. Instead, such providers — whether offering communications tools, hardware, or software — are considered engaged in trade. Because these technologies do not maintain an account relationship with users or have access to their crypto assets, they are excluded from Bank Secrecy Act obligations. This same logic underpins decentralization goals: the control test offers objective, measurable criteria for assessing the extent to which third parties provide essential network services.

Example Implementation:

> *The source code of the blockchain network enables participants in the blockchain network to maintain total independent control of network tokens and other digital assets owned by them, with access and management governed solely by their private keys.*

Discussion of Limits and Potential Carveouts: One question we received was around the scope of the application of this principle to L2 bridges. L2s are still mostly early in the decentralization journey but they, along with other protocols, should benefit from transition relief once we set legislative and regulatory targets to work toward. We generally believe that Stage 2 L2s should receive some measure of regulatory accommodation. Ultimately regulatory agencies should provide more guidance and ruling making with respect to how this principle should be applied in the L2 context.

5. Distributed Blockchain Network

Principle: No person or group has unilateral authority to alter the network or control a large percentage of network tokens.

This principle adjudges the practical concentration of power of the initial development team and other market participants. Such actors may retain or accumulate power by controlling consensus mechanisms — for example, through large-scale mining operations or, in proof-of-stake systems, by holding a significant portion of staked tokens. Similarly, governance token holders with controlling stakes can disproportionately influence the outcome of governance votes.

Policy Rationale: If a network can be unilaterally altered by a person or group under common control, the potential for information asymmetries, conflicts of interest, insufficient disaffiliation, and value extraction is significant. Beyond ensuring that no person can unilaterally change the functionality or operation of a network, decentralized blockchain networks should seek to incentivize participants to contribute value to the ecosystem and correspondingly distribute that value more equitably among system stakeholders according to their contributions.

If a network can be unilaterally altered by a person or group under common control, the potential for information asymmetries, conflicts of interest, insufficient disaffiliation, and value extraction is significant.

To achieve this, blockchain networks need to vest meaningful power, control, and ownership with system stakeholders. As a consequence, the value of the ecosystem as a whole accrues to a broader array of participants rather than one central entity and its shareholders. This helps to transform networks from proprietary technologies to public infrastructure, thereby reducing control-related risks to tokenholders.

The broadly distributed threshold of 20% is meant to drive the distribution of tokens among stakeholders (i.e., developers, contributors, and consumers) to incentivize contributions to the network for the benefit of all. In other words: facilitating the benefits of modern network effects, without the pitfalls of centralized control and captive economies. We believe that this principle should also be reflected in regulations that address secondary market actors because, as pointed out by various critics, equality of access in principle means being susceptible to capture in practice.

This principle, as it relates to an initial issuer group, was proposed in the Financial Innovation and Technology for the 21st Century Act in 2023, which specified a threshold of 20%, and can be traced back to the 2019 Framework's criteria and Hester Peirce's Token Safe Harbour Proposal 2.0. The paper *Reframing How We Look at a Crypto Legislative Solution* engages in a broader discussion of how market actors can amass power over the means of consensus and network infrastructure and pose a risk to network resiliency.

Example Implementation:

> *No person or group of persons under common control: (a) have the unilateral authority, directly or indirectly, to alter the functionality, operation, or rules of consensus or agreement of the blockchain network; or (b) beneficially own, in the aggregate, 20% or more of the total amount of units of a network token or had the unilateral authority to direct the voting, in the aggregate, of 20% or more of the outstanding voting power of such network token.*

Discussion of Limits and Potential Carveouts: During discussions with industry, many suggested that "common control" should be interpreted consistently with its meaning under securities law, particularly in light of concerns that tokenholder governance models could be construed as de facto general partnerships. In this context, we noted that token voting alone — absent collusion or a formal relationship — should not, by itself, trigger a finding of common control.

This principle should draw rational lines between the initial developer group and large passive holders in assessing concentration.

It should not disincentivize the sustainability or continued development of a network, and related, it should recognize the need to create carveouts for independent treasuries and practical guidance for token supply models with inflationary mechanics.

Credible neutrality is one of the core advantages of open blockchain networks over closed systems.

6. Credibly Neutral Blockchain Network

Principle: The source code does not empower specific persons with private permissions over others.

Policy Rationale: Credible neutrality is one of the core advantages of open blockchain networks over closed systems. Because blockchain networks can offer transparent, enforceable guarantees about how they operate, they minimize the risk of discrimination against specific users or use cases. This ensures the network remains open and accessible to all. In contrast, the absence of credible neutrality inherently creates a dynamic where certain users or applications are favored over others, fostering information asymmetries and enabling value extraction. By establishing a level playing field, credible neutrality promotes fair competition, broad participation, and ultimately maximizes the network's value for all users.

Example Implementation:

> *The source code of the blockchain network does not empower specific persons with private permissions, hard-coded privileges, or similar rights over other similarly situated persons.*

Discussion of Limits and Potential Carveouts: Consistent with a few other principles, the concerns industry stakeholders raised on credible neutrality were mostly limited to the need for safety carveouts and for the practical implementation of this principle being easiest at the infrastructure level and more nuanced at the application level.

7. Economically Independent Blockchain Network

Principle: Mechanisms that facilitate value accrual to network tokens should be functional.

Policy Rationale: Given that network tokens derive their value from the operation of an underlying blockchain network, it is critical that such value-driving mechanisms be deployed to reduce control-related risks to network tokenholders.

A blockchain enabling the redemption of network tokens for digital products or services (e.g., paying for gas fees on a layer-one blockchain) is the simplest example of economic independence. Though simple, its impact is exceedingly effective — this step alone can embed supply and demand drivers into the system's network token.

While providing an economic model may make it easier to demonstrate that tokenholders have a "reasonable expectation of profits" when they acquire a network token, an economic model reduces risks associated

Implementing a token economic model is a critical step in aligning profit expectations with the functioning of the blockchain network rather than with a centralized company.

with such expectations — where a centralized team with control of the system has yet to deploy such mechanisms, the economic functioning of the system will be entirely speculative, and the network token's value will be much more susceptible to information asymmetries, market manipulation, and value extraction driven by incentive misalignment among network participants. Where an economic model has been deployed, such control-related risks are greatly reduced.

Ultimately, implementing a token economic model is a critical step in aligning profit expectations with the functioning of the blockchain network rather than with a centralized company. This helps establish the network token's economic independence from any operating entity, thereby mitigating control-related risks such as information asymmetries. Moreover, economic independence can reduce the likelihood that the token will be classified as a "convertible virtual currency" or that its issuer will be deemed a money transmitter.

Example Implementation:

> *The primary programmatic mechanisms of the blockchain network that are intended to facilitate substantial value accrual to its network tokens through the functioning of such system are functional, including, without limitation, mechanisms that: (a) enable the use, consumption or redemption of such network tokens for the digital products or services offered via the blockchain network; (b) automatically adjust the supply of the network token; or (c) programmatically distribute proceeds from the functioning of the blockchain network.*

Discussion of Limits and Potential Carveouts: Industry stakeholders frequently brought up the role of decentralized governance in the ability to update or alter the value accrual mechanisms.

Additional Considerations and Carveouts

1. Application of the Principles Above the Base Layer

We think the above principles should be most stringently applied to the base layer of blockchain networks. However, for L2s and decentralized applications, which derive their fundamental security and integrity from the underlying base layer, different weights should be assigned to the principles depending on context — for example, one could place

greater emphasis on trustlessness, permissionlessness, and autonomy, and a more flexible approach to distribution and credible neutrality.

Practical realities — including operational needs, distinct threat models, and the specific functions served by higher layers — should inform a tailored but coherent application of these principles. Materiality should also guide flexibility: centralized features should be evaluated based on whether they materially affect the system's core functioning, or whether they relate to ancillary services that do not alter fundamental trust assumptions.

Accordingly, carveouts and accommodations should include narrowly tailored security and emergency mechanisms, structured transition periods for existing networks, and frameworks should be created for regulators to recognize and support credible progressive decentralization paths for emerging systems.

2. Decentralized Governance Carveout

As a more general matter, nothing in the framework is intended to freeze or ossify the technology, particularly when upgrades are necessary to enhance user safety or improve the user experience. The legislative framework should: (i) affirm that governance mechanisms and, where appropriate, delegations to trusted parties for user safety, are permissible; and (ii) direct regulatory agencies to provide guidance on governance standards, including the circumstances under which governance may delegate authority to trusted parties, and the criteria such parties must meet.

With respect to point (ii), an example implementation for such a carveout could be: *A Network shall be deemed to have achieved [the foregoing control test] notwithstanding any delegation of authority with respect to the functioning of such Network to a [decentralized governance system] so long as any such delegation is limited in scope and purpose to protect users and in line with general market practices, including, without limitation, delegation of special powers to a security council in the event of an emergency incident.*