Designing Policy for a Flourishing Blockchain Industry

Decentralization Research Center

February 2025

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.

The Decentralization Research Center would like to thank Miles Jennings, Sarah Brennan, and Thomas Chow for their contributions and assistance on this report.

Cover photo: Artem Krapivin

Table of Contents

Introduction

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, easy 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 which provide significant autonomy and economic opportunity to users. The worst case 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.

A key challenge for policymakers is that there is no universally accepted definition for a decentralized blockchain or digital asset, but over the past several years, academic research and industry experience have helped us to better understand where to draw the line. Based on our review of relevant literature and work in the industry, we believe that focusing on control is the most effective option for defining decentralization. We propose eight criteria below that, if met, would significantly reduce information asymmetries stemming from the control of a blockchain's token, justifying lower regulatory burdens or exemptions under securities laws. We would greatly appreciate any feedback from the community on these criteria.

These criteria, or a subset thereof, could be used as standards to meet a decentralization test in regulatory safe harbors, like the Safe Harbor 2.0 proposed by SEC Commissioner Hester Peirce, or legislation that classifies different types of digital assets, like the Financial Innovation and Technology for the 21st Century Act (FIT 21). We believe these criteria provide an objective basis for measuring control, rather than relying solely on a subjective, principles-based approach, which has proven to be too ambiguous for builders to rely upon and could be weaponized by future SEC leadership.

The most effective way for policymakers to understand and define decentralization is to focus on control.

We believe that it is not necessary to use all of these criteria in all cases, as there should be a path to compliance for all types of blockchain projects. However, these criteria 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 criteria are designed to be objective and rules-based, rather than principles-based, to ensure greater certainty and scalability. They are also technology-neutral across distributed ledger technologies and evergreen, meaning any current or future blockchain network can meet the standard. The criteria were designed such that verification would rely primarily on the network's source code, with additional transparency provided through mandatory disclosures when necessary. A blanket carveout/exception for decentralized governance should also be included.

The SEC is emerging as the first mover in developing blockchain rules and, conveniently, decentralization complements their mission to

protect investors and maintain fair markets. Commissioner Peirce's proposed Safe Harbor 2.0 provides a strong foundation for a framework that distinguishes between different types of blockchain networks while promoting the transparency and accountability the industry needs. In the coming weeks, the Decentralization Research Center, alongside aligned organizations, will publish in-depth recommendations for regulators and policymakers, aiming to help them craft policies that enable the industry to reach its potential.

Control Criteria for Decentralization

1. Open Blockchain Network

> *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).*

Closed software systems operated by centralized companies subject their users to a number of risks – the source code is not made available to users, and users cannot operate the code themselves. 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. Open-source requirements are an essential factor in establishing a standard for reducing control and ensuring that intellectual property rights do not provide indirect mechanisms of control that enable value extraction from token holders. Additionally, they enable participants to fork the underlying blockchain, and the transparency of the source code enables anyone to verify how it functions, including that the system can operate without human intervention and that no person has inherent authority to make unilateral decisions impacting the functioning of the source code.

The criteria for Open Blockchain Networks was originally proposed in Defining Decentralization for Law in 2020.

2. Functional Blockchain Network

> *The blockchain network is functional, enabling participants to transact through the updating of the state of the blockchain network, including, but not limited to, by: (a) transmitting and storing value; (b) participating in staking or other method of securing the blockchain network; (c) participating in services provided by or an application running on the blockchain network; or (d) participating in any decentralized governance system.*

When a blockchain network is not functional (or not yet functional), it and any token related thereto are inherently controlled by any person whose efforts are required to make it functional, thereby exposing network tokenholders to significant control-related risks, including those stemming from the manual performance of operations and the risks of potential mistakes in calculation or data storage. Additionally, a nonfunctional system requires the substantial efforts of others to maintain current and future operations – subjecting any such system to significant risks of information asymmetry.

Functionality should be a prerequisite for any control-based decentralization threshold.

Accordingly, functionality should be a prerequisite for any control-based decentralization threshold. A functionality requirement does not need to rise to the level of requiring a project's entire development roadmap be achieved, but does require baseline functionality as described above, which every project should be capable of satisfying.

This criterion was originally proposed 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 focused on systems being "fully developed and operational" and that network tokens be usable inline with their "intended functionality."

3. Autonomous Blockchain Network

> *The blockchain network operates, executes and enforces its operations and transactions without human intervention,*

functioning solely on pre-established, transparent rules encoded directly within the source code of the blockchain network.

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 one node or participant goes offline or is compromised, the system continues to function because the control is distributed across numerous nodes — autonomous functioning reduces the risk of systemic failure or attack, as there's no central target for malicious actors. 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.

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 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.

4. Permissionless Blockchain Network

The blockchain network does not empower any person or group of persons under common control with unilateral authority to restrict or prohibit lawful 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.

If a tokenholder's use or participation in a blockchain network can be unilaterally restricted, then the tokenholder 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. Further, permissionlessness is the foundation upon which greater decentralization can be achieved through organic system growth over time. By enabling any third party to interact and build on top of the system, trust dependencies on the original development team are greatly reduced and should naturally reduce further over time, thereby continuing to mitigate risks associated with information asymmetries. While some projects will be able to start out permissionless, for many projects permissionlessness at early stages would introduce security risks and is therefore better introduced when the project is more mature. It could therefore be counterproductive to require such criteria at the launch of a project, but reasonable to apply it prior to insiders selling.

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

5. Non-Custodial Blockchain Network

> *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.*

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.

Thus, technologies that are non-custodial ensure that only the user can make decisions and take actions such as the movement or transfer of crypto assets. This criteria is well-informed by the above-mentioned

guidance and codified at 31 CFR § 1010.100(ff), stating that technology simply providing "the delivery, communication, or network access services" used to support a user's activity is not a financial intermediary but rather such suppliers of these tools (communications, hardware, or software) are engaged in trade. Authorities exclude such non-custodial products and technology from Bank Secrecy Act obligations because there is no control over activities in situations where the software or network does not have an account relationship with the user or access to an owner's crypto assets. The same reasoning applies to decentralization goals — the control test offers objective and easily measurable criteria to determine the degree to which third parties provide essential network services.

6. Distributed Blockchain Network

> *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, [10-20]% 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 [10-20]% or more of the outstanding voting power of such network token.*

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

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.

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 10-20% 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 have not yet settled on a specific percentage but have included that range as it represents the outer limits of what is generally discussed.

This criterion was originally 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. Further, definitions of "control" under securities laws have long focused on ownership thresholds in the 10% to 20% range.

7. Credibly Neutral Blockchain Network

> *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.*

Credible neutrality is one of the key benefits of open blockchain networks over closed corporate networks. Inherently, because blockchain networks can make guarantees about how they will function, they can remove the possibility of unfair discrimination against particular users and use cases, thereby ensuring that the system remains open and available to all. Meanwhile, a lack of credible neutrality inherently pits one user/use case against others, thereby creating incentives for information asymmetries and value extraction to arise. By creating a level playing field, credible neutrality fosters competition and enables all persons to benefit from participating in the system, thereby maximizing the potential value of the system for all users.

Credible neutrality is one of the key benefits of open blockchain networks over closed corporate networks.

8. Economically Independent Blockchain Network

> *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.*

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-1 blockchain) is the simplest example of economic independence. Though simple, in execution 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 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, the implementation of a token economic model is a fundamental step to squarely anchoring profit expectations to the functioning of the blockchain network, as opposed to a company — it makes the network token economically independent of any operating company, thereby reducing control-related risks, including information asymmetries. In addition, economic independence will help to reduce the risk that a given network token may be deemed a "convertible virtual currency" and that its issuer may be deemed to be a money transmitter.