Stellar

Whitepaper

DESIGNING A PRACTICAL FRAMEWORK FOR DECENTRALIZATION

WHAT IS DECENTRALIZATION?

Decentralization is a way to classify how a system operates. In general, a system that is "decentralized"[1] operates through a series of rules that coordinate the contributions of diffuse individual components, or nodes. These nodes are self-organized, and interactions among nodes collectively achieve the system's goal without the need for a central guiding or authoritative entity. As such, each node is responsible for contributing to the purpose of the system and one node or component cannot operate the system independently.

In the case of blockchain, this purpose could be verifying and recording transactions. In open blockchains, that verification is not done by an individual or affiliated group of users, but by a network of independent computers that each act as nodes of the blockchain. These nodes interact and make decisions collectively through a consensus process. No single entity owns or controls the network, and power and trust are distributed among its users. A blockchain can successfully operate in this decentralized way because of protocols that establish the underlying set of rules and standards that define how each node will function and, in turn, how the network will function.

WHAT IS THE IMPORTANCE OF PROTOCOLS TO DECENTRALIZED SYSTEMS?

As alluded to above, decentralization does not imply a lack of order or structure simply because the network has no reliance on a central authority. In fact, decentralized networks are rules-based, highly organized systems and because these networks rely on code, not humans, to run them, they are more predictable. Protocols dictate how the network operates and how participants in consensus communicate and interact with one another, meaning that governance is embedded into network design. A network's consensus mechanism serves to enforce those rules and guidelines, and does so in a clear and transparent manner for network participants. Unlike traditional centralized systems, where a single entity creates and enforces the system's rules, decision-making in decentralized systems is distributed among participants. Validators have a central role, deciding on block validity. Depending on the protocol, token holders or even general users may also have governance or voting rights. In general, in a decentralized system, individual actions are consequential to the system in which they participate and participants are incentivized to act in a way that serves the collective good: maintaining a secure, trustworthy, and rules-based system.

[1] Decentralization and disintermediation are terms that are often–but mistakenly–used interchangeably. While decentralization delegates decision-making away from a central authority, disintermediation refers to the reduction or removal of intermediaries. For example, disintermediated finance removes the intermediary in a transaction, allowing for things like peer-to-peer payments that do not require the use of a bank.

While decentralization may seem novel, decentralized networks already serve an important place in society. For example, the Internet was created as an open, decentralized communications network with its own set of protocols that are still used today. The U.S. Department of Defense designed the Internet as a decentralized system to ensure resiliency in the face of a nuclear attack: even if an attack were to bring down a portion of the network, its decentralized nature would allow operations to continue.

WHAT DISTINGUISHES DECENTRALIZED NETWORKS FROM CENTRALIZED ONES?

In a centralized system, the behavior of a network is orchestrated by a central influence or control. This is in contrast to a decentralized system, in which there is no central coordinating or governing unit. However, decentralization and centralization are not binary. Instead, decentralization-centralization should be understood to be a spectrum; neither is absolute. Blockchain networks may have some dimensions that are decentralized, and others that are more centralized. These dimensions are rarely static, and may become more decentralized or centralized over time as a network and its ecosystem evolves.

We can observe this spectrum of centralization-decentralization in other real world contexts, like political systems. For example, governance in India is highly centralized, and many local budget allocations are decided by the central government. Conversely, in Sweden, a decentralized governance model allows local authorities to have more discretion over community affairs. Another example of this spectrum is in organizational structure within firms. Newer, smaller companies tend to divide teams by function, and those functions then report to a central leader. As companies mature, develop, and increase in size, some firms will opt to move to a more decentralized model, where teams are divided by product or problem and are composed of members from multiple functions. These decentralized teams allow for greater resiliency and scalability.

WHY DECENTRALIZATION?

Decentralization is an emerging tool in finance although it is not a new concept. It allows for:

Operational resilience:

Decentralization offers an important enhancement over traditional technology: robust core operations. Centralized networks rely on a single actor or set of specific actors to maintain the network, manage participants, and set or alter rules. This reliance can lead to systemic failures, like bottlenecks, outages, or inefficient service. Decentralized systems reduce such operational risks because there is no single point of failure. They also improve network security by decreasing the potential impact an attack can have on the system.

Data integrity:

Decentralization in blockchain networks supports data integrity in three key ways. First, there are multiple copies of the data across the network. Any attempt to represent an altered copy as authentic is obvious because it conflicts with the replicated copies. Second, use of public key encryption allows for inexpensive verification of data and imposes impossibly high costs for forgery on anyone who does not hold the matching secret key. Third, decentralized blockchain networks require multiple parties to validate data as part of a transparent consensus process before adding that data to the immutable ledger, making it impossible for a single entity to unilaterally alter and manipulate data. As a result, data remains accurate, complete, and consistent across all nodes.

Trust minimization:

The decentralization of trust represents a profound change to the financial ecosystem. In the banking sector, for example, users place trust in banks–centralized entities–to process transactions and hold records, and each bank has full discretion to determine whether to provide accounts or loans to its prospective customers. With decentralization, no single entity owns or controls a decentralized network, and trust is therefore distributed across the network. Trust is not placed in a single person or organization, but dispersed across the community. Further, participants in a decentralized system do not need to trust a single entity or group of entities to allow them access. Because decentralized systems allow for open participation, no single actor or group of actors has the authority to act as a gatekeeper.

HOW DO WE DESIGN A PRACTICAL FRAMEWORK FOR DETERMINING DECENTRALIZATION?

We appreciate the efforts in the United States, European Union, and elsewhere to develop a comprehensive understanding of what constitutes a decentralized network and to lay out basic criteria for decentralization. Creating a meaningful framework for what determines a network's degree of decentralization will help provide regulatory clarity and support the growth and development of the blockchain industry as a whole.

Given the varied and novel aspects of blockchain-based technology, a one-size-fits-all approach to determining decentralization is neither appropriate nor practical. We therefore caution against creating an overly-prescriptive definition of "decentralization" because the blockchain industry is nascent, and will continue to develop and evolve over time; many of the fundamental assumptions that hold now will become outdated. For instance, much of the current literature on determining the degree of decentralization specifically relies on interpreting proof-of-work (PoW) and proof-of-stake (PoS) mechanisms[2]. However, this methodology is limiting and will be inapplicable as new consensus mechanisms are developed. There are already alternative consensus mechanisms that move away from a simple distribution of nodes or staked tokens, and relying on indicators relevant only to PoW or PoS to determine a network's decentralization are not relevant to these alternative models.

[2] PoW and PoS are the two major consensus mechanisms that blockchain networks use to verify new transactions and add them to the ledger. PoW uses a competitive validation method to confirm transactions and add new blocks to the ledger. PoS uses randomly selected validators to confirm transactions and create new blocks.

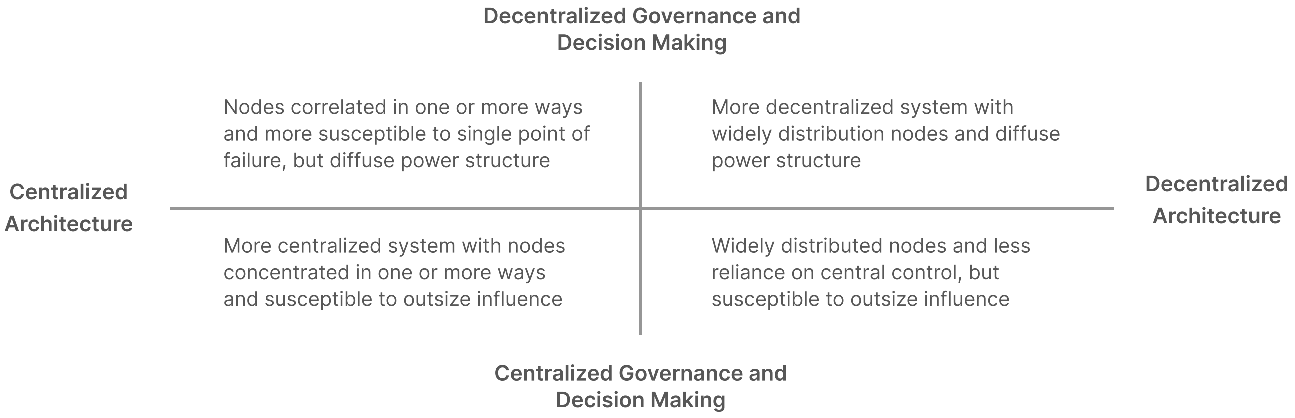
WHAT DO WE RECOMMEND?

We recommend the development of a straightforward, multi-factor framework for evaluating a network's degree of decentralization, one that allows regulators the ability to evaluate specific attributes of a network and its underlying protocol. A broad framework that draws on high-level principles allows for adaptability avoids a situation in which strict criteria developed today fail to capture future innovations. Such a framework positions policymakers and regulators to address fundamental questions about whether a network has characteristics of centralization, such as:

- Is the network governed by a single entity or affiliated group?
- Is there a risk of collusion or concentration of power among a few participants in the network?
- Can one or more participants acquire enough influence to compromise the decision-making protocol in the network and have outsize power?
- Is there any single point of failure in the system?
- Is the decision-making process for initial and ongoing design decisions open and inclusive?
- Can anyone participate in the validation process without explicit permission?
- Can all participants – ordinary users and validators – freely join and leave the network?
- Does the network accommodate participation from a diverse set of stakeholders?

To help answer these questions, we created a simplified framework that isolates two key dimensions of decentralization and gives policymakers the tools to quickly determine where a network falls on the decentralization-centralization spectrum. We recognize that other dimensions of decentralization exist beyond the two we have identified, and that nuance is lost in developing simplified evaluation criteria. However, a highly complex framework would be incompatible with easily administered policies and would be burdensome to apply in practice. We therefore recommend a streamlined, practical framework that can be applied to any blockchain network, regardless of consensus mechanism. Because some systems are designed to become more decentralized over time, the framework may indicate centralization in one or both dimensions if applied early in a network's development. The framework therefore captures only a moment in time, and should be reapplied as a network matures.

	Definition	Metric
Decentralization Dimension		
Architecture	This dimension assesses the distribution of power and decision-making authority within the network. It evaluates the likelihood of centralized power among a limited number of participants. This process can be unintentional and organic, or facilitated by malicious actors that aim to influence protocol changes solely to benefit themselves. This dimension also evaluates whether a protocol's design motivates participant coalescence. As governance converges on a network, select participants accumulate outsize influence in decision-making and the system is no longer decentralized.	Measuring a system's robustness in the face of correlated failures can help determine that system's degree of architectural decentralization. The severity and likelihood of correlated failures can be evaluated by assessing concentration risk in key areas, such as the following: • Geographic (ex: node operators are concentrated in a single region) • Network (ex: nodes are reliant on a limited number of cloud providers)
Governance and Decision Making	This dimension measures whether the number of systems involved in a blockchain network are sufficiently distributed so that there are limited points of failure. A higher degree of architectural decentralization implies a more resilient system: even if one or more systems crash, the network continues to operate.	The Nakamoto Coefficient[3] represents the minimum number of nodes required to disrupt a blockchain network. The larger the Nakamoto Coefficient, the more decentralized the network's effective operational governance is.



Decentralized Governance and Decision Making

Nodes correlated in one or more ways and more susceptible to single point of failure, but diffuse power structure

More decentralized system with widely distribution nodes and diffuse power structure

Centralized Architecture

Decentralized Architecture

More centralized system with nodes concentrated in one or more ways and susceptible to outsize influence

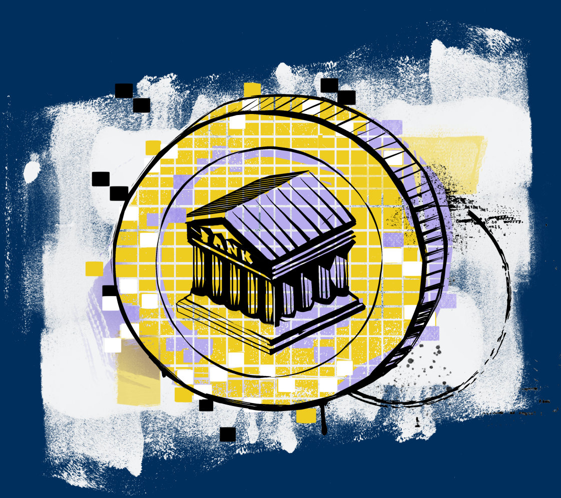
Widely distributed nodes and less reliance on central control, but susceptible to outsize influence

Centralized Governance and Decision Making

[3] We acknowledge that the Nakamoto Coefficient is a simplistic metric for determining a network's degree of governance and decision-making decentralization. Active research is underway within the Stellar Development Foundation to develop a rigorous, quantitative framework for evaluating governance, but this is a longer-term process. In the interim, however, the Nakamoto Coefficient serves as a practical heuristic, one that provides a high level impression of the distribution of power and decision-making authority on a network.

WHAT DOES DECENTRALIZATION MEAN FOR REGULATION?

Building consensus around what decentralization is – and is not – and how to determine whether a network is decentralized lays the groundwork for developing appropriate regulatory approaches. With centralized systems, policymakers are charged with assessing whether a central authority operates responsibly and transparently. Laws, regulation, and rules condition the behavior of central authorities and engender trust with system participants. But decentralization allows for an alternative model of trust, one that does not depend on centralized authority. Decentralized systems are designed so that no single actor or affiliated group can exert undue influence or control over the system, and it is the protocol that conditions the behavior of participants in the system. In a truly decentralized system, trust is shifted away from a centralized authority and to the system itself.



In decentralized systems, policymakers must assess whether a decentralized system's underlying protocol eliminates the risks associated with centralized authority. Where decentralized systems do not eliminate or sufficiently mitigate risks associated with centralized authority, oversight and regulation should follow. For example, if there is a security vulnerability in a protocol that is exploited, how is that vulnerability addressed? If there is a risk of collusion among entities running nodes, how can that risk be alleviated? Regulation can solve for these gaps in trust. Further, an advantage of decentralized blockchain networks is that the technology itself can achieve regulatory compliance and supervision objectives. The use of a shared, trusted ledger is an important innovation that allows for real-time monitoring and reporting.

Ensuring consumer and investor protections, promoting market integrity, and mitigating systemic risks remain key priorities for policymakers, whether looking at centralized or decentralized systems. Yet decentralization raises fundamental questions about the nature of regulation, and how that regulation is deployed most effectively. In confronting this unfamiliar territory, policymakers will be challenged to rethink the very nature of oversight.