Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains—An Agent-Based Simulation Approach

Article in European Journal of Information Systems · January 2024

DOI: 10.1080/0960085X.2022.2125840

Christoph Mueller-Bloch
ESSEC - Ecole Supérieur des Sciences Economiques et Commerciales

Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach

Christoph Mueller-Bloch
ESSEC Business School
muellerbloch@essec.edu

Jonas Valbjørn Andersen
IT University of Copenhagen
jova@itu.dk

Jason Spasovski
ZTLment
jason@ztlment.com

Jungpil Hahn
National University of Singapore
jungpil@comp.nus.edu.sg

July 21, 2022

Forthcoming in the
EUROPEAN JOURNAL OF INFORMATION SYSTEMS

Understanding Decentralization of Decision-Making Power in Proof-of-Stake Blockchains: An Agent-Based Simulation Approach

Abstract

Blockchain systems allow for securely keeping shared records of transactions in a decentralized way. This is enabled by algorithms called consensus mechanisms. Proof-of-work is the most prominent consensus mechanism, but environmentally unsustainable. Here, we focus on proof-of-stake, its best-known alternative. Importantly, decentralized decision-making power is not an inherent feature of blockchain systems, but a technological possibility. Numerous security incidents illustrate that decentralized control cannot be taken for granted. We therefore study how key parameters affect the degree of decentralization in proof-of-stake blockchain systems. Based on a real-world implementation of a proof-of-stake blockchain system, we conduct agent-based simulations to study how a range of parameters impact decentralization. The results suggest that high numbers of initial potential validator nodes, large transactions, a high number of transactions, and a very high or very low positive validator network growth rate increase decentralization. We find weak support for an impact of changes in transaction fees and initial stake distributions. Our study highlights how blockchain challenges our understanding of decentralization in information systems research, and contributes to understanding the governance mechanisms that lead to decentralization in proof-of-stake blockchain systems as well as to designing proof-of-stake blockchain systems that are prone to decentralization and therefore more secure.

Keywords: *Blockchain, consensus mechanism, centralization, decentralization, decision-making power, governance*

1. Introduction

Since their inception (Nakamoto, 2008), blockchain systems have gradually achieved mainstream recognition, and their potential to fundamentally affect organizations, industries, and economies is now widely acknowledged (Beck et al., 2018; Clemons et al., 2017; Risius & Spohrer, 2017). While historically shared records of transactions would be kept by a centralized authority or institution, the main value proposition of blockchain systems is to securely keep shared records in a decentralized way (Constantinides et al., 2018). To function without a designated central operator, a blockchain system requires a protocol to generate consensus among the nodes that jointly administer the blockchain, which is an append-only, distributed database (Lumineau et al., 2021; Rossi et al., 2019; Zachariadis et al., 2019). This so-called consensus mechanism (or consensus protocol) sets the basic rules by which a node is selected to decide on the contents of a block (which contains an array of transaction records) that is added to the blockchain (Bano et al., 2017; Tschorsch & Scheuermann, 2017). Some of the most prominent consensus mechanisms include proof-of-work (PoW) and proof-of-stake (PoS). In PoW, the main determinant of the right to validate the next block is the amount of computing power a node possesses (Nakamoto, 2008). In PoS, the right to validate the next block is determined primarily by the proportion of cryptocurrency a node owns (King & Nadal, 2012). PoW is widely criticized for its high energy costs without external utility and associated environmental and other welfare concerns (Benetton et al., 2021). In response, PoS is increasingly gaining ground. In 2019 and 2020, more blockchains based on PoS than on PoW were launched, making PoS the most common consensus mechanism in new blockchain systems (Irresberger et al., 2021). Moreover, prominent blockchain systems such as Ethereum are in the process of migrating to PoS at the time of writing.[1] In this paper, we therefore focus on PoS, which has received little attention in prior research, despite its importance in practice.

Consensus mechanisms such as PoW and PoS are not only meant to facilitate coordination and thereby agreement among the nodes; they are also designed with the intention of ensuring a high degree of decentralization of the right to decide on the content of blocks. Decentralization implies that decision-making power (or control) is more dispersed across a larger group of individuals, whereas centralization implies that decision-making power is concentrated in a single person or a small group (King 1983). Despite the intent of achieving decentralization, consensus mechanisms do not necessarily guarantee decentralization in practice. In other words, decentralization is not an inherent feature of blockchain systems, but a desired outcome (Cong et al., 2021; Halaburda & Mueller-Bloch, 2020). The reason decentralization is desirable is that highly centralized decision-making power in blockchain systems gives rise to a major security threat, the so-called 51% attack. In a 51% attack, a malicious node obtains a majority of the decision-making power and uses its power to compromise the integrity of the blockchain. This is not just a theoretical concern: 51% attacks are becoming increasingly frequent in practice (Shanaev et al., 2019). Overall, centralization of decision-making power in blockchain systems causes the technology to lose its main value proposition of ensuring the integrity of shared records without the need for trusted third parties, since it implies that a single entity can gain the ability to compromise the integrity of the blockchain. Even if that entity were non-malicious, its power would require all other system participants to trust its benevolence. Therefore, centralization is a major factor that might prevent

[1] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

blockchain technology from realizing its aspired potential of making trusted third parties redundant.

The critical role of the distribution of decision-making power in blockchains prompts us to study how decentralization, or centralization, simultaneously emerges from both node behavior and the consensus mechanism. While previous research has studied the specific trade-off between coin inflation and decentralization of PoS blockchains (Irresberger, 2018), so far there is no comprehensive study on how changes in a number of different key parameters impact decentralization in PoS blockchains. We study this issue by adopting a complex adaptive systems (CAS) perspective. The CAS framework is a powerful tool to study how the micro-level interaction of agents within a system environment results in emergent outcomes at the macro level (Holland, 1992; Miller and Page, 2009). It is regularly used in information systems research (e.g., Haki et al., 2020; Nan, 2011; Zhang et al., 2020) to study settings with high complexity. We conceptualize blockchain systems as CAS, in which blockchain nodes are represented as agents within the environment of a blockchain system, that interact based on rules specified by a PoS consensus mechanism. We rely on an agent-based simulation to study how changes in node behavior (transaction amount, transaction volume, and network growth) and the setup of blockchain systems (initial network size, initial stake distribution, transaction fees) affect the distribution of decision-making power in blockchain systems and thus their integrity. The agent-based simulation is validated using real-world data from NXT, the first blockchain system based on PoS.

We find that a high number of initial potential validator nodes, large transactions, and a high number of transactions increase the degree of decentralization. Our results also suggest that a very high or very low positive network growth rate increases the degree of decentralization.

We only find weak support for an impact of changes in transaction fees and initial stake distributions on the degree of decentralization. Based on our analysis, we can derive concrete measures for blockchain system design to address the risk of overtly centralized decision-making power in PoS blockchain systems. Our study is one of the first in information systems research to look at the blockchain protocol. While there are many studies focusing on blockchain applications, few have investigated how to design blockchain systems as such (Rossi et al., 2019). In doing so, our paper fills a major gap: achieving decentralization is critical to ensure the security and trustworthiness of blockchain systems.

The remainder of this paper is structured as follows. In section two, we introduce the prior literature on centralization, decentralization, and PoS blockchain systems. In section three, we introduce the CAS framework that we adopt to study blockchain consensus mechanisms. In section four, we describe the agent-based model of the PoS consensus mechanism, discuss its validation and the simulation procedure. In section five, we present the results of the simulation experiments and further scenario testing. In section six, we discuss the findings and conclude the paper.

2. Background

In this section, we provide a brief overview of prior information systems research on centralization and decentralization and explain how the emergence of blockchain systems changes how we view these concepts. Subsequently, we discuss the importance of decentralization for blockchain systems, provide an overview of threats associated with centralization, and position this study in the context of extant literature on blockchain systems.

2.1. Centralization and Decentralization of Information Systems

While information systems research has held a keen interest in centralization and decentralization for many decades, the interpretation of these concepts has not always been fully consistent (Ein-Dor & Segev, 1978). Importantly, centralization and decentralization have often been conceptualized as multidimensional, covering not only how decision-making power is allocated, but also other aspects, for instance the geographical location of computing equipment (Ein-Dor & Segev, 1978; King, 1983). In this paper, we use the terms centralization and decentralization only to refer to the dispersion of decision-making power.[2]

Historically, research focused on whether the use of computers would centralize or decentralize organizational decision-making power. The large and expensive mainframe computers that characterized the early days of computing were thought to favor centralization. Later, as computers became smaller and less expensive over time, there was an expectation this would further decentralization. As distributed computing became increasingly common, it became clear that the computing architecture by itself would not necessarily preordain centralization or decentralization (Bloomfield & Coombs, 1992). Research focus then shifted to why organizations would choose certain governance arrangements, including centralization or decentralization, and how and why these arrangements would lead to certain organizational outcomes (King, 1983; Sambamurthy & Zmud, 1999; Weill & Ross, 2004). More recently, the

[2] A recent paper argues that there has been some confusion regarding the distinction between *decentralization* and *distribution* (Vergne, 2020). Therefore, we will also clarify how we use the term *distribution* in this paper. First, we use the term to describe computing environments that rely on multiple computers that are connected on a network (such as distributed systems and distributed databases). Note that such distributed computing architectures do neither preordain centralization or decentralization (of decision-making power). Second, we use the term to refer to how a resource is dispersed across a population (as in wealth distribution or income distribution). In this paper, we focus on the distribution of decision-making power among computing nodes. Note that the use of the term distribution does not imply *how* decision-making power is dispersed—for this we use the terms centralization and decentralization. While our use of the term differs from Vergne's (2020), it adheres to long-established norms in computer science and economics.

increased need to coordinate across organizational boundaries, brought about by emergence of digital platforms and ecosystems, has reinvigorated the debate on the centralization and decentralization of decision-making power. However, this literature stream also views centralization or decentralization primarily as a means to an end (Tiwana et al., 2010).

In the realm of blockchain systems, the role of centralization and decentralization is fundamentally different. Here, decentralized decision-making power is not a means to achieve a goal. Conversely, it is the goal. This is because the idea behind blockchain systems is to eradicate the need for trusted third parties that wield centralized decision-making power. Prior to the emergence of blockchain systems, such trusted third parties were typically taken for granted. For instance, central banks would manage monetary policy, and centrally-controlled online marketplaces would support transactions among parties that do not trust each other and often do not even know each other. The advent of blockchain systems has challenged this status quo, promising to fundamentally disrupt and transform many societies and industries (Beck et al., 2018; Catalini & Gans, 2020; Clemons et al., 2017; Risius & Spohrer, 2017).

Another difference to established information systems research on centralization and decentralization lies in the organizational setting. Prior research on centralization and decentralization focused on traditional organizations (King, 1983; Sambamurthy & Zmud, 1999; Weill & Ross, 2004) and digital platform ecosystems (Tiwana, 2010). Blockchain systems represent a very different type of organizational setting: they are distributed systems, in which participants are not governed by managers, but by a software protocol. This means that the scope of their potential decisions is very restricted, and the source of decision-making power is clearly specified: in blockchain systems, the protocol that governs interaction provides clear rules regarding the distribution of decision-making power (Andersen & Bogusz, 2019; Hsieh et al., 2018; Rossi et al., 2019). Nodes can primarily exercise their decision-making power by deciding about the contents of a block that is to be added to the blockchain (Bano et al., 2017; Tschorsch & Scheuermann, 2017). Conversely, in traditional organizational settings, the scope of potential decisions would be vast, and the origins of decision-making power would be multifaceted and ambivalent (Bloomfield & Coombs, 1992; Markus & Bjørn-Andersen, 1987).

2.2. Centralization and Decentralization in Blockchain Systems

Technically, a blockchain is a distributed transactional database that is governed by a consensus mechanism (Constantinides et al., 2018; Rossi et al., 2019; Zachariadis et al., 2019). Blockchain transactions are stored in batches called *blocks* (which may also be empty). The database is distributed across a number of agents called *nodes* (Nakamoto, 2008). Blockchains are different from traditional distributed databases in that they can function without a designated central operator. This requires a mechanism that incentivizes agreement among the nodes, thereby avoiding the creation of competing blockchains (i.e., forks). This is achieved by consensus mechanisms, which provide the basic rules with regard to the distribution of decision-making power across the nodes. The node that obtains the decision-making authority, the *validator node*, obtains the right to decide on the content of the next block that is added to the blockchain (Bano et al., 2017; Tschorsch & Scheuermann, 2017). For every new block to be added to the blockchain, decision-making power is recalculated based on the specifications in the consensus mechanism. This introduces a degree of randomness and serves to disperse decision-making power. How decision-making power is obtained varies across different consensus mechanisms (Bano et al., 2017; Bonneau, 2018).

In this paper, we focus on PoS, a consensus mechanism that was devised to address environmental concerns related to PoW. The latter was proposed by Nakamoto (2008) to enable consensus in the Bitcoin blockchain. PoW allocates decision-making power mainly based on a competition of who can solve a cryptographic hash puzzle the soonest. Due to the preimage resistance of cryptographic hash functions, the likelihood of winning the competition is proportional to a node's expenditure of computing power. In practice, this led to a computational arms race. For Bitcoin alone, the energy consumption is comparable to that of a small, industrialized country (Saleh, 2021). PoS, the most salient current alternative to PoW (Irresberger et al., 2021), addresses this issue by distributing decision-making power mainly based on the size of nodes' investment (i.e., the "stake") in the cryptocurrency associated with the blockchain. Nodes with larger stakes therefore are more likely to obtain more decision-making power (Bano et al., 2017; King & Nadal, 2012).

A high degree of centralization of decision-making power is highly problematic since a node with particularly high decision-making power can compromise the integrity of the blockchain. By monopolizing the right to decide upon the content of new blocks, a malicious node could perform a 51% attack. For instance, the attacking node could claim all transaction fees, perform double spending, or reject or include transactions as preferred (Conti et al., 2018). Overall, centralization is associated with three major threats (see Table 1). First, a node might perform a 51% attack to gain utility *within* the blockchain system. For instance, the node might want to achieve monetary gain by double-spending cryptocurrency (Nakamoto 2008). It has been argued that this type of attack is not very likely: a powerful node might gain more utility from not attacking, since an attack would undermine the validity of its wealth (Kroll et al., 2013). However, recent evidence suggests that such attacks take place frequently, which might be explained by the fact that cryptocurrency value only decreases moderately (12 to 15 percent) in the case of such attacks (Shanaev et al., 2019). In Table 1, we term this attack as the *Nakamoto* *attack*, since this type of 51% attack is described in Nakamoto's white paper (2008). Second, a node might perform a so-called *Goldfinger attack* to gain utility *outside* of the blockchain system (Kroll et al., 2013). There are three conceivable reasons for conducting this type of 51% attack. One potential reason for a Goldfinger attack might be a government or another institution wanting to achieve some institutional goal, for instance related to law enforcement. Alternatively, a non-state attacker might want to attain some political or social goal, for instance in a social protest. Finally, an attacker might seek financial gain outside of the blockchain system, for instance after having taken short positions on the blockchain system's cryptocurrency. Overall, it has been argued that Goldfinger attacks are not an unlikely scenario (Kroll et al., 2013), in particular since decision-making power need only be acquired temporarily as well, not necessarily permanently (Bonneau, 2018). The third threat posed by centralization is a scenario in which a non-malicious node gains a lot of decision-making power so that it possesses the capacity to conduct a 51% attack. While the node is non-malicious and therefore has no intention to attack, the sheer possibility may already have detrimental effects on the blockchain system due to a lack of trust. For instance, other potential validator nodes might leave the system and investors might decide to sell their cryptocurrency. While this scenario has been described (Halaburda & Mueller-Bloch, 2020), we are not aware of any research demonstrating this empirically. Overall, our discussion of the three different threats shows that centralization always poses a threat to blockchain systems, regardless of whether or not the node with a high degree of decision-making power is malicious. Moreover, it is not possible for a malicious node to attack the system as long as the system is sufficiently decentralized. Therefore, in this paper we do not focus on whether or not individual nodes are malicious, but whether or not the blockchain system is decentralized.

Table 1. Blockchain Centralization and Associated Threats

Threat	Description	Assumptions
Nakamoto attack	A node with a high degree of decision-making power attacks the blockchain system to gain utility within the blockchain system (Nakamoto, 2008).	The node is malicious and maximizes utility *within* the blockchain system by conducting a 51% attack.
Goldfinger attack	A node with a high degree of decision-making power attacks the blockchain system to achieve an extrinsic goal (Kroll et al., 2013).	The node is malicious and maximizes utility *outside* of the blockchain system by conducting a 51% attack.
Centralization vulnerability	A node possesses a high degree of decision-making power, thereby creating a vulnerability that can have detrimental effects for the blockchain system (Halaburda & Mueller-Bloch, 2020).	Blockchain users are aware of the centralization and consider it a threat.

Other threats specific to PoS-blockchains exist, such as the "Nothing-at-Stake" attack, in which nodes extend every potential fork (Bano et al., 2017). We follow Bonneau (2018) and Saleh (2021) in assuming that a solution exists for these attacks. Bonneau (2018) assumes that a takeover requires that a single node obtains a majority of the overall stake in the blockchain. However, while in PoS-blockchains the main determinant of decision-making power is the stake a node holds, the actual selection of the validator node (and hence the degree of decentralization) is determined by the combination of stake held by the node together with other parameters built into the consensus mechanism which only materializes at runtime. We therefore devise a separate measure for decision-making power in this paper, based on a real-world implementation of a PoS consensus mechanism. Moreover, despite being named 51% attack, we do not assume that there is a specific amount of decision-making power a node needs to obtain to compromise the blockchain (e.g., 51 percent), given that the greater the relative decision-making power the node obtains, the more likely it is that the attack succeeds (Bonneau, 2018). In line with this notion, we conceptualize decision-making power as a continuum, in which a higher degree of decentralization ensures a higher degree of integrity.

In this paper, we focus on the (de-)centralization of decision-making power related to transaction validation. However, other dimensions of decision-making, and therefore centralization or decentralization, are also associated with blockchain systems, thereby introducing potential single points of failure (Halaburda & Mueller-Bloch, 2020; Sai et al., 2021). For instance, the initial system development (Beck et al., 2018) and system update development (Azouvi et al., 2018) are often marked by centralization in practice. While some kinds of centralization may in fact be beneficial (e.g., Cennamo et al., 2020), there is reason to believe that not only centralization of transaction validation, but most kinds of centralization undermine blockchain's promise of removing trusted third parties. For instance, if there was only a single person or a small group doing development work, they could introduce backdoors, which could corrupt the integrity of the system if appropriate monitoring by outsiders was lacking.

Our paper contributes to the literature on blockchain consensus mechanisms. So far, most of this literature has focused on PoW blockchains. Papers focusing on this consensus mechanism include Gervais et al. (2016), Arnosti and Weinberg (2019), Biais et al. (2019), Alsabah and Capponi (2020), Benetton et al. (2021), and Cong et al. (2021). However, few papers have focused on PoS blockchains. Irresberger (2018) conducts a simulation study of the trade-offs between coin inflation and the degree of decentralization in PoS blockchains. He does not consider cases in which transaction fees are the only block reward, arguing this may undermine consensus (Carlsten et al., 2016). However, a recent paper by Saleh (2021) demonstrates that in PoS, as opposed to PoW, consensus is more likely with low block rewards. This is because low block rewards shift validator incentives towards maximizing coin value, which encourages consensus. Consequently, we focus on PoS blockchains without inbuilt inflation, in which transaction fees are the only block reward, thereby complementing the study by Irresberger (2018). Our analysis also goes beyond the study by Irresberger in that we investigate the impact of changes in a number of different key parameters on decentralization, instead of focusing on one specific trade-off. Our results do not generally apply to stake-based on-chain blockchain governance, which has recently become more common (Tsoukalas & Falk, 2020), but only to the PoS consensus mechanism.

3. Complex Adaptive Systems Modeling of Proof-of-Stake Blockchain Systems

So far, we have discussed the proof-of-stake consensus mechanism based on a review of the current literature. This has provided a qualitative description of the phenomenon under study. To study how the degree of decentralization emerges as a result of interactions among nodes, we need an analytical tool specifically suited for multi-level quantitative theorizing. Such a tool is provided in the complex adaptive systems (CAS) framework. The CAS framework allows for studying emergent outcomes of interactions within PoS blockchain systems since it captures how rule-based interactions among individual agents, that is, interactions between nodes governed by the PoS consensus mechanism, result in emergent outcomes at the global system level, that is, the distribution of decision-making power in the blockchain system. A complex adaptive system is defined as being "…composed of interacting agents described in terms of rules..." (Holland, 1995, p. 10). The CAS framework has been applied in a wide variety of fields ranging from biology, physics, and healthcare (Peters, 2014) to information systems (Nan, 2011; Haki et al., 2020; Zhang et al., 2020).

In this research, we leverage the CAS framework and its associated computational instruments (e.g., Miller & Page, 2009) to study how interactions among nodes in a PoS blockchain system result in emergent outcomes related to the distribution of decision-making power. By applying the CAS framework, we can identify the impact of specific design choices and behavioural scenarios on the degree of decentralization.[3] This necessitates a framework capable of accommodating the design and behavioral parameters of blockchain systems as well as accounting for the rules embedded in the consensus mechanism itself. The CAS framework conceptualizes complex adaptive systems in terms of the structural levels of a system at large and in terms of the components necessary for generating and perpetuating emergent outcomes (see also Table 2).

The structural levels of a CAS include generative structures, elemental structures, and observed structures (Drazin & Sandelands, 1992). First, generative, or 'deep', structures refer to the tacit rules that govern actions of and interactions between actors. These structures are the unobserved, generative, and recursive functions that produce elemental and observed structures. Second, elemental structures include the states of agents and their actualized interactions. These states and interactions produce micro-level structures that can be observed in time and space. Although there is no universally agreed-upon paradigm for describing the elemental structures of a CAS (Gell-Mann, 1994), three components have been consistently recognized as the core of the theory: agents, interactions, and environment (e.g., Holland, 1995; Nan, 2011). Agents are the basic entities in complex adaptive systems. Depending on the phenomenon under study, they can be representations of, for instance, individuals of a species of animals, organizations, technologies, individual human beings in a social setting, or nodes in a blockchain system. Agents are characterized by a set of attributes and a number of behavioral rules. Attributes refer to parameters that can be defined at the agent level and that define the identity or state of an

[3] A natural experiment could potentially also be suitable to study how changes in behavior and design choices affect the degree of decentralization of decision-making power. However, using the CAS perspective in conjunction with agent-based simulations has the advantage of allowing for probing several interventions in parallel and affording control with respect to the kind of intervention being studied.

agent. Behavioral rules specify how each agent interacts with other agents or with input from the model environment. Interactions consist of mutually adaptive behaviors manifested through structural connections between agents through which flows of resources are channeled. The environment represents the medium for agent interaction and is characterized by a structural topography in terms of gradients related to resource distribution and possibilities for interaction. Finally, observed structures refer to the social facts that emerge at the macro-level from interactions between agents. Even though each agent is oblivious to the properties and behavior of the system, the aggregation of their interactions results in emergent system outcomes (Holland, 1992). Applying the framework of CAS to study blockchain systems, we can now summarize the structure, components, and elements of CAS. Table 2 provides a summary of the CAS framework and exemplifies each of its components in the blockchain context.

Table 2. Conceptualizing Blockchains as CAS

CAS Structure	CAS Component	CAS Model Elements	Equivalent in Proof-of-stake Blockchain Systems
Generative structure (unobserved)	*Model Rule*	The behavioral logic of the model specified at the model-level	Consensus mechanism as an algorithm for choosing the validator node
Elemental structure (micro-level)	*Agent*	Identity	A public address that identifies nodes
		Attributes	Currency stake
		Behavioral rules	Make a transaction
	Interaction	Connection	Transactions on the blockchain, fee paid to winning validator node
		Flow	Amount and volume of currency transactions between agents, e.g., nodes' stakes decrease when making a payment
	Environment	Initial conditions, model parameters, and parameter settings	Number of available validator nodes, initial distribution of stake
Observed structure (macro-level)	*Emergent property*	Output observations at the system level	Distribution of decision-making power, structure of the validation network

4. CAS Instrument: Agent-Based Modeling

The agent-based modeling (ABM) approach allows researchers to probe distributed systems and explore how its agents interact at different parameter settings to produce emergent structures and behaviors over time. ABM has been used as an analytical tool for studying social behavior since Schelling's (1969) study of segregation and has increasingly gained attention as a method for generating theory in the social sciences (Bonabeau, 2002; Epstein, 2006). The value of ABM as a tool for quantitative theorizing in information systems and management research has previously been demonstrated by Nan and Tanriverdi (2017), Rivkin and Siggelkow (2007), and Siggelkow and Levinthal (2003), among others.

Extending from its roots in CAS theory, the general idea of ABM is to specify agents within a system environment and endow them with simple theory-based interaction rules and then observe the emergent macro-level outcomes (Holland, 1995; Miller & Page, 2009). Agent-based models can in principle be expressed as a series of mathematical equations. Complex agent-based models are usually expressed in computational processes and are studied using numerical (e.g., Monte Carlo) methods (Epstein, 2006).

4.1. Modeling Decision-Making Power through the PoS Consensus Mechanism

We conceptualize a blockchain system as a CAS of agents (i.e., nodes participating in a blockchain network) in which emergent decisions are made about who gets to validate a block. To ensure the agent-based model reproduces the behavior of a blockchain system with a high degree of fidelity, we followed the general procedure for validating an agent-based simulation model suggested by Klügl (2008). The procedure focuses specifically on establishing face validity as well as calibrating and validating the model empirically (the latter is described in section 4.3). To establish face validity and to validate the simulation empirically by comparing the outcomes of the simulation with the real-world implementation, we require a real-world implementation of a PoS blockchain as a baseline. We chose the NXT blockchain[4] since it

[4] https://nxtplatform.org/

represents a rather prototypical and straightforward implementation of a PoS blockchain system. In particular, in NXT decision-making power does not increase the longer tokens have been in a node's account (this is known as *coin age*). Moreover, as one of the first PoS blockchains, at the time of writing NXT has already been running for over six years without any major bugs, suggesting that this is a well-designed implementation of a PoS blockchain. To ensure face validity, we built the simulation model by translating salient features of the Java source code of the actual open-source NXT implementation directly into Python (see Appendix A). This ensures that the mechanisms of the simulation model align mechanically with the empirical context it reproduces.

We model the blockchain system as containing A_t potential validator nodes at any point in time t; the initial number of potential validator nodes is A_0. The blockchain system is an open network in which new nodes can freely join the network. The growth of the network is modeled as simple exponential growth using parameter G, which denotes the growth rate – $A_{t+1} = A_t \cdot (1+G)$. Each node a is assigned a unique identifier and possesses a currency balance b_{at} at time t; a node a is assigned an initial currency balance b_{a0}. As the PoS consensus mechanism relies on the currency balance of each node b_{at} to determine its decision-making power, the initial distribution of stake balances across all nodes B is a key parameter as it effectively determines how decentralized decision-making power in the system is at the onset. For each block (or time t), each node can be in one of two states s_{at}, since it can either be the validator node of the block, or not. A node a obtaining the authority to validate a specific block at time t (here determined by each block) would have state $s_{at} = 1$, and the remaining nodes (a') would be assigned state $s_{a't} = 0$).

As previously described, the PoS consensus mechanism distributes decision-making power among agents. The decision-making power distribution is defined as *P*(*A*). To correct for fluctuations in the demand for block validation, that is, spikes and dips in transactions sent per block, the PoS consensus mechanism sets a multiplier M_t that is determined by the amount of time it took to validate the previous block. Moreover, to further increase decentralization of decision-making power, each node is assigned a validation threshold hit_{at}, which is a randomly generated value unique to each node at time *t*. The model can then determine the decision-making power p_{at} of a node *a* at a point in time *t*. This is determined by the product of the global demand multiplier M_t and the node-specific effective balance b_{at} divided by the validation threshold hit_{at} for node *a* at time *t*. Consequently, the decision-making power p_{at} of each node *a* at each block *t* is defined by:

$$p_{at} = \frac{M_t \times b_{at}}{hit_{at}}$$

The node with the highest decision-making power p_{at} becomes the validator node for the respective block and is assigned validation state $s_{at} = 1$. The validator node then receives the transaction fee *f*, which is added to its effective balance b_{at}. The transaction fee *f* is paid by all transacting nodes for each block. The transaction fee amount for each block depends on the average transaction fee *F*. We assume that all eligible nodes are in principle willing to validate transactions, since once a node possesses cryptocurrency, there is little additional cost associated with becoming a potential validator node (only an Internet connection is needed), but substantial potential benefit exists in the form of transaction fees. Having specified how the model determines the decision-making power for each agent, we now turn to explaining how the distribution of decision-making power emerges over time from node interactions governed by the PoS consensus mechanism.

The distribution of decision-making power emerges as a result of redistribution of stake through transactions, which is determined by the transaction volume, the amount of currency sent in each transaction, and the transaction fees. Transactions between nodes in the system are modeled so that for each block (i.e., time step t in the model), a number between 0 and A transactions between randomly selected node pairs take place. The transaction volume parameter is denoted by V. Together with the transaction amount, defined in the model as the average amount of stake sent in each transaction and denoted by U, and the average transaction fee denoted by F, it affects the redistribution of effective balance between nodes in the blockchain system. This redistribution affects the distribution of stake, which in turn affects the distribution of decision-making power in the blockchain system at large. Table 3 shows an overview of model parameters as well as agent states for the agent-based simulation of the PoS consensus mechanism.

Table 3. Parameters for Agent-Based Simulation of the PoS consensus Mechanism

Parameter	Description	Notation
Model Parameters		
Initial number of nodes	The initial number of agents available as potential validator nodes (i.e., active and online agents)	A_0
Validation multiplier	A multiplier based on the time it took to validate the previous block	M
Transaction fee	The average transaction fee acquired by the validator node	F
Initial stake distribution	Initial distribution of stake across agents set to either the observed NXT distribution or any of a range of common distributions	B
Transaction amount	The average amount sent for each transaction between agents	U
Transaction volume	Number of transactions between agents	V
Blockchain network growth rate	Multiplier for the growth of the number of potential validator nodes in the network	G
Agent States		
Validation state	Binary indicator of whether an agent has validation rights or not	s_a
Effective balance	The balance of currency for each agent	b_a
Validation threshold	A randomly generated value that is unique to each agent	hit_a
Decision-making power	Determined by the global demand multiplier, the validation threshold, and the effective balance of each agent	p_a

4.2. Measuring the Distribution of Decision-Making Power

To measure centralization or decentralization of decision-making power, we require a measure that allows quantifying how decision-making power is distributed among the agents that are part of the network. We use a measure of inequality, which can be defined as the dispersion of a distribution of population attributes (Litchfield, 1999). Inequality measures are often used to quantify how income or other welfare indicators are distributed (ibid). We use an inequality measure to assess how decision-making power is distributed. There are several inequality measures, most prominently entropy-based measures, such as the Theil index and the Gini coefficient.

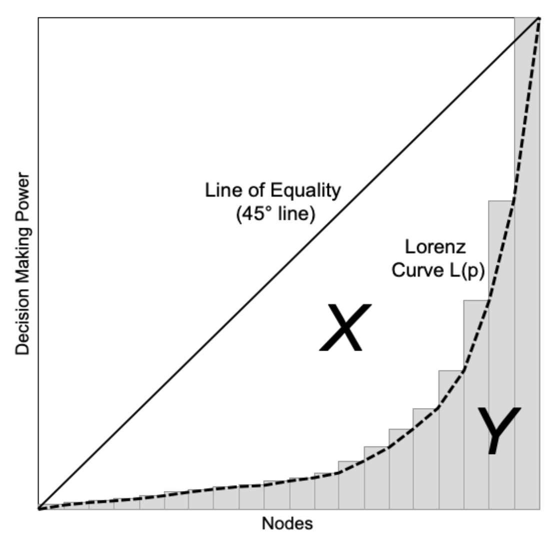
Both the Theil index and the Gini coefficient adhere to critical principles, in particular mean independence, population size independence, symmetry, and Pigou-Dalton Transfer sensitivity (World Bank Institute, 2005). Mean independence implies that the measure would not change if the population attribute measured (in our case, decision-making power) would be doubled for all agents. For the blockchain context, this means that the measure should not change if the decision-making power of all nodes were to be doubled. Population size independence means that the measure would not change if the population size were to change. This means that changes in the number of potential validator nodes should not affect the measure. Symmetry implies the measure would not change if two agents swapped their fraction of the population attribute (i.e., decision-making power). For our context, this implies that the nodes' identity should be irrelevant for the measure. Pigou-Dalton Transfer sensitivity means that transferring a fraction of the population attribute (i.e., decision-making power) from powerful to less powerful agents would reduce the measure (ibid). In the blockchain validation context, this means that the transfer of decision-making power from powerful to less powerful nodes should lead to a decrease in the measure, indicating a reduction of centralization. Even though both Theil index and Gini coefficient fulfil these four criteria, they are also marked by differences. Importantly, the interpretation of the Gini coefficient is more intuitive since it is calculated using the Lorenz curve (Lerman & Yitzhaki, 1984). Due to its superior interpretability, we therefore rely upon the Gini coefficient to measure the distribution of decision-making power.

The Gini coefficient uses the Lorenz curve as the basis for its computation. As illustrated in Figure 1, the Gini coefficient is defined (and calculated) as the ratio of the area *X* between the line of equality (i.e., the 45° line) and the Lorenz Curve L(p) to the area *X*+*Y* under the line of equality (which is 0.5) (Gastwirth, 1972). For discrete distributions, the Gini coefficient can be computed as:

$$Gini = \frac{X}{X+Y} = 1 - \frac{Y}{X+Y} = 1 - 2 \times \sum_{a=1}^{A} \left(\frac{A-1-a}{A+1} \right) \times \left(\frac{p_a}{P} \right)$$

where *P* is the sum of all nodes' decision-making power.

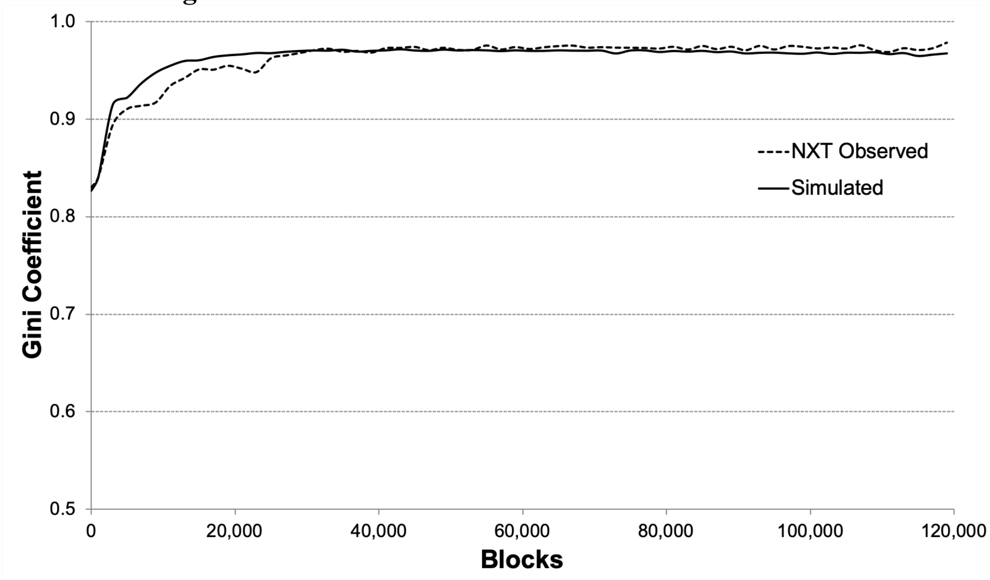
Figure 1. The Gini Coefficient and Lorenz Curve



4.3. Simulation Model Calibration and Empirical Validation

Having replicated the observed source code and specified the outcome variable of the distribution of decision-making power, we then calibrated and empirically validated the simulation model. To calibrate the model, its parameters have to be set in a way that a structurally correct model produces a valid outcome (Klügl, 2008). We ran the simulation model with the initial parameter settings observed in the actual NXT blockchain and compared the outputs of the observed versus simulated blockchain systems in terms of distribution of decision-making power as measured by the Gini coefficient. We collected transaction data for the initial 120,000 blocks of the NXT blockchain and measured how the distribution of decision-making power changed over time (see Figure 2). We then used the actual observed parameter values of the NXT blockchain system as a baseline to calibrate the simulation model. Specifically, the simulation model used the observed NXT blockchain system data—the initial number of nodes (A_0) was set to 73, the average transaction fee amount (F) to 414 units of currency, the average transaction amount (U) to 39,434 units of currency, average transaction volume per block (V) to 2.54, and the blockchain network growth rate (G) to 0.03. We chose to validate our simulation model against the first 120,000 blocks of the NXT blockchain (equivalent to approximately 125 days), since after 120,000 blocks, the NXT blockchain system's consensus mechanism was altered. To ensure that our simulation results reflected the underlying structure of the model rather than a particular realization of a stochastic process, we performed 20 replication runs for each setting and calculated the average. We then took the moving average with a window size of 20 blocks to smoothen out fluctuations and highlight longer-term trends.

Figure 2. Observed versus Simulated Gini Coefficients



Comparing the results of the simulated Gini coefficients against the actual NXT data, we find that the simulation model after an initial discrepancy converges on a decision-making power distribution similar to the NXT blockchain system (see Figure 2). The initial difference between the simulated and observed distribution of decision-making power can be explained by the fact that the average amount sent per transaction was larger by a factor of ten for the initial 25,000 blocks of the observed blockchain compared to the remaining 95,000 blocks. This can be ascribed to the extraordinary dynamics in the genesis of the NXT blockchain system rather than to a general mechanism of the PoS consensus mechanism.

4.4. Simulation Experiments

Having validated our agent-based model, we moved on to simulate the effects of changes in relevant simulation parameters (see Table 4) on the decentralization of decision-making power. We used the parameter settings observed in the NXT blockchain system to establish our simulation baseline. This is to ensure that any subsequent experimental treatments are based on reasonable and realistic values and to allow for discerning the effects of parameter manipulations. We then manipulate each of these parameters with a range of 7 relevant values ranging from 5 to 1,000 percent of the corresponding baseline value (i.e., 5%, 10%, 25%, 50%, 250%, 500% and 1,000% of the baseline value). There are two exceptions here. First, we fixed the validation multiplier parameter (*M*) to the model baseline value as it represents the demand for validation that is determined by exogenous drivers. Second, the initial stake distribution parameter (*B*) concerns a matter of kind and not a matter of quantity. Hence, it is not possible to manipulate it using fractions or multiples of a baseline value. Instead, we manipulate the initial stake distribution parameter with various canonical distributions (e.g., uniform, normal, bimodal, power law, etc.) to analyze the impact of changes in the initial stake distribution on the decentralization of decision-making authority.

We repeated this for all parameters settings to perform a complete sensitivity analysis of the main effects each of the parameters has on the distribution of decision-making power. Having observed the main effects of each parameter in the sensitivity analysis, we then simulated relevant scenarios based on high-impact parameter settings to further explore the implications of the sensitivity analysis. In total, we performed 880 runs across 120,000 simulated time steps per run (i.e., blocks). The actual values tested in the simulation experiments are summarized in Table 4.

Table 4. Experimental Design – Parameters Simulated

Design Parameters								
Initial stake distribution (*B*)	Observed	Normal	Power-Law 1	Power-Law 2	Bimodal Beta	Uniform	Skewed	NA
Treatment relative to baseline	*5%*	*10%*	*25%*	*50%*	*Baseline*	*250%*	*500%*	*1,000%*
Initial number of nodes (A_0)	4	7	18	37	73	183	365	730
Transaction fee (*F*)	21	41	104	207	414	1035	2070	4140
Behavioral Parameters								
Transaction amount (*U*)	1,972	3,943	9,859	19,717	39,434	98,585	197,170	394,340
Transaction volume (*V*)	0.13	0.25	0.64	1.27	2.54	6.35	12.7	25.4
Blockchain network growth rate (*G*)	0.0015	0.0030	0.0075	0.0150	0.0300	0.0750	0.1500	0.3000

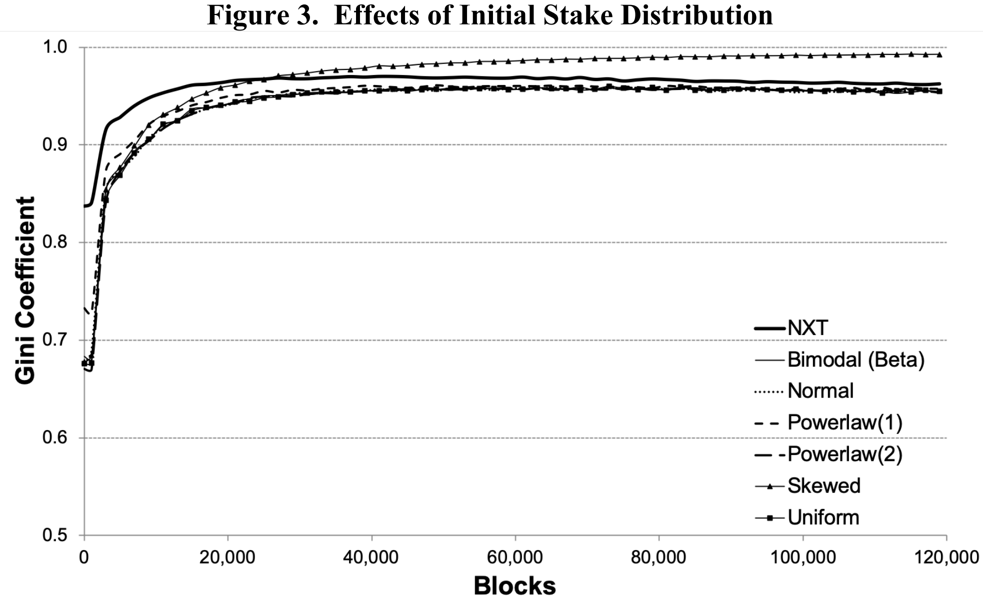
5. Findings

Our analysis shows that the distribution of decision-making power in the observed NXT blockchain system is highly centralized with a Gini coefficient above 0.95 after the initial 25,000 blocks representing the genesis of the blockchain (see Figure 2). This begs the question of how to increase decentralization (i.e., reduce centralization) in order to promote the integrity of the blockchain. In the following, we discuss how changes in model parameters affect the degree of decentralization of decision-making power.

5.1 Initial Stake Distribution

To discern how the distribution of decision-making power is affected by the initial distribution of stakes among nodes, that is, the distribution of cryptocurrency across all nodes, categorical treatments depending on the specific distribution were required. As such, we tested six of the most common distributions along with the observed distribution from the validation data set, a normal stake distribution, two power-law distributions with opposite orientations, that is, with both many 'poor' with few 'rich' and many 'rich' with few 'poor' nodes, a bimodal beta distribution, a uniform distribution where all nodes are given equal stakes, as well as a skewed distribution in which one agent holds 90% of the initial stake. Figure 3 shows how, beyond some initial disparity, all initial stake distributions except the skewed distribution converge on a somewhat stable Gini coefficient of around 0.95, matching the observed NXT distribution. The skewed distribution is designed so that one node is initially assigned 90% of the total stake, with the remaining 10% distributed equally among the remaining nodes. In this case, the blockchain network converges on complete centralization, that is, the initially dominant node consistently wins validation rights. Similar results for the majority of initial stake distributions indicate that, while given vastly different initial distributions, the consensus mechanism redistributes stake over time in such a way that the initial stake distribution, in all but the case of the skewed distribution, has relatively little impact on the distribution of decision-making power. This can be explained as a consequence of the randomness introduced to the blockchain by the PoS consensus mechanism implementation in the form of the random validation multiplier and continuous transactions between nodes.

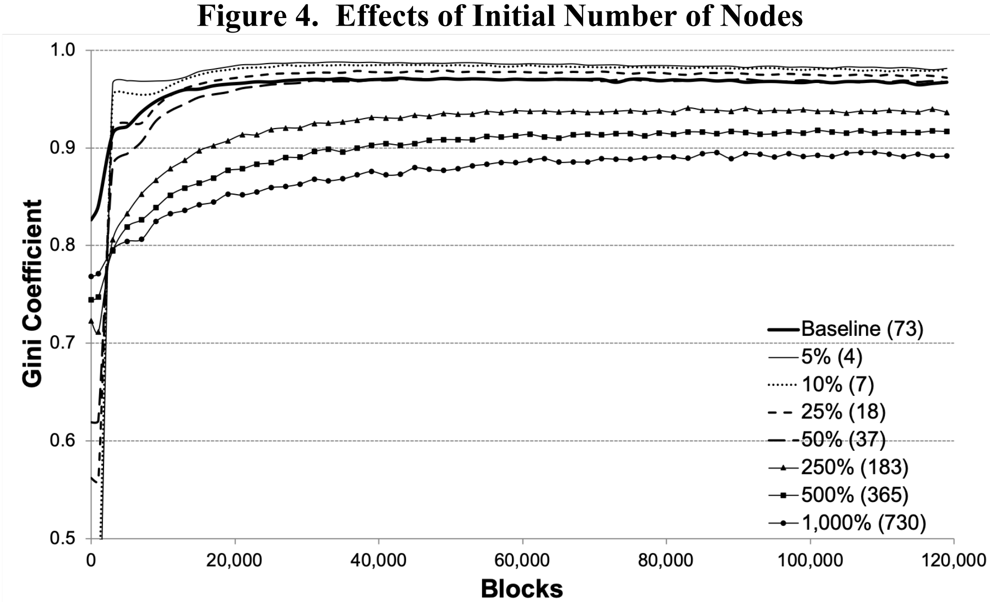
Figure 3. Effects of Initial Stake Distribution



5.2. Initial Number of Nodes

The initial number of nodes denotes the number of potential validator nodes available at the genesis of the blockchain. Because nodes receive a transaction fee that effectively increases their stake and thereby their chance of obtaining the right to validate blocks, the size of the initial blockchain system can be influential in the distribution of decision-making power throughout the evolution of the blockchain. Figure 4 shows that a low number of initial nodes result in very low decentralization of decision-making power, whereas decentralization increases as the number of initial nodes increases. Effectively, in order to achieve substantial decentralization of decision-making power, the blockchain system should be initiated with a greater number of potential validator nodes, all else being equal. This result has implications for the timing of when a PoS blockchain system should be launched, since a premature initiation with few potential validator nodes reinforces the dynamics leading to lower decentralization. This also implies that PoS blockchain systems with smaller numbers of initial validator nodes are generally more prone to breaches of integrity.

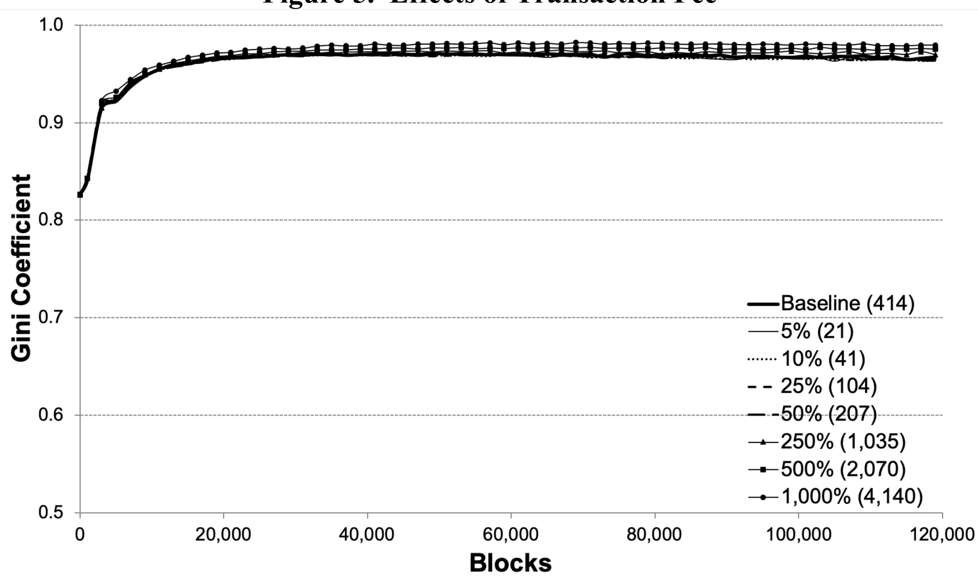
Figure 4. Effects of Initial Number of Nodes



5.3. Transaction Fee

Higher transaction fees should intuitively mitigate centralization by incentivizing a larger number of potential validator nodes to participate early on in the lifespan of a blockchain system. However, as shown in Figure 5, the sensitivity analysis for the parameter denoting the average transaction fee for each block reveals only modest effects of changes in the average transaction fee on the distribution of decision-making power. Increased transaction fees have a slightly negative effect on decentralization, as shown in Figure 5. In the context of the PoS consensus mechanism, this negative effect could be explained by the fact that the validator node for each block is primarily selected based on its currency stake so that the winning validator node is more likely to accumulate even larger stakes from increased transaction fees and thereby, in turn, increase its future decision-making power.

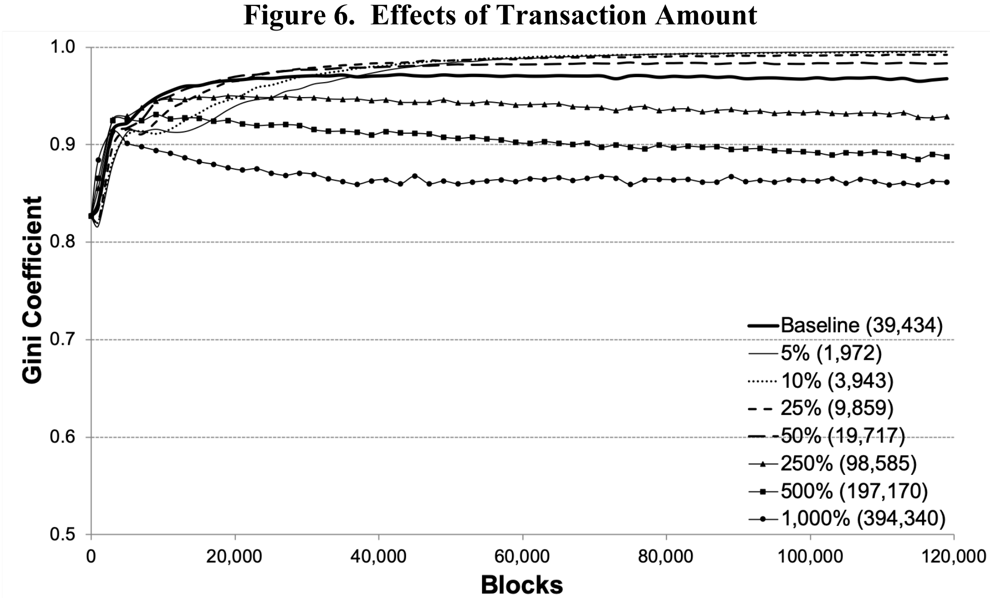
Figure 5. Effects of Transaction Fee



5.4. Transaction Amount

Similarly, large average transaction amounts could mean that stake, and thereby decision-making power, would accumulate in the hands of a few nodes. However, as illustrated in Figure 6, higher average transaction amounts positively affect decentralization. It should be noted that for the settings at which the degree of decision-making power decentralization starts to substantially increase (i.e., at a threshold of 250 percent of the observed value), transaction amounts are quite substantial—for 250 percent of the observed value, transactions equal to an average amount of at least 98,585 units, equivalent to USD 4,478 per transaction (using the median exchange rate during the first 120,000 blocks of the NXT blockchain). Even larger average transaction amounts lead to even higher degrees of decentralization. The transaction amount is determined by agent behavior rather than by blockchain design and is therefore not directly available for manipulation by those designing and managing the blockchain system. However, issues of application context become salient, given that blockchains used in contexts operating with small transaction amounts (e.g., retail, payments) might be more vulnerable than blockchains with mostly large transactions (e.g., financial settlement, assets).

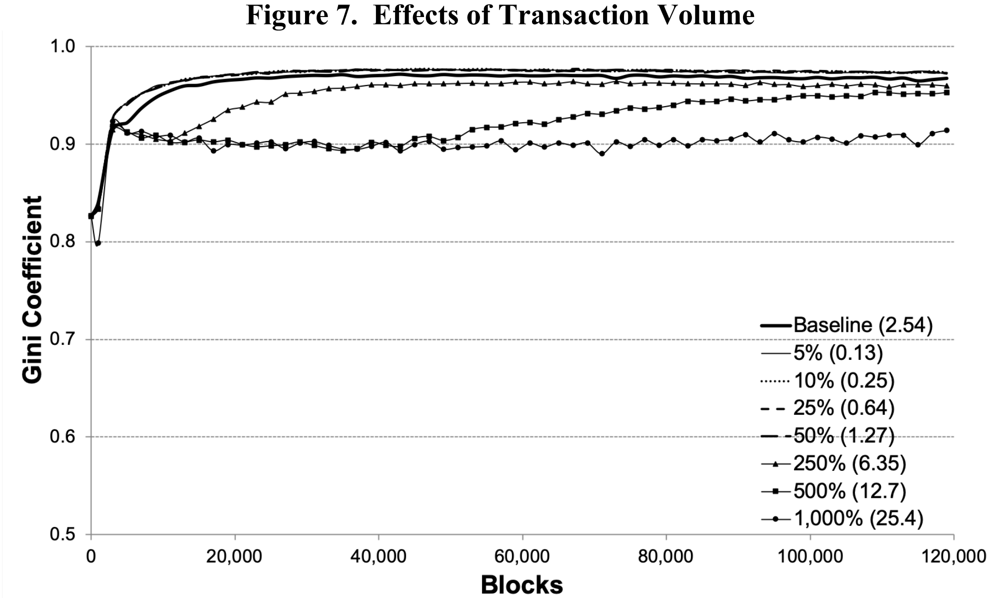
Figure 6. Effects of Transaction Amount



5.5. Transaction Volume

Another model parameter determined by agent behavior is the transaction volume in terms of the average number of transactions per block. The sensitivity analysis for this parameter shows a positive effect of increases in transaction volume on decentralization of decision-making power (see Figure 7). However, the distribution of decision-making power over time converges to a level at which only a slight positive effect remains. There seems to be a positive relationship between average transaction volume and the time it takes for that convergence to take place, as illustrated in particular by the behavior of the graphs indicating the degree of decentralization at the levels of 250 percent and 500 percent of the observed value. The graph illustrating the degree of decentralization at the levels of 1,000 percent of the observed value presumably exerts similar behavior, only with a greater delay, given that it takes an increasing trend as time passes, similar to the behavior of the two aforementioned series (i.e., at 250 and 500 percent of the observed value) right before they converge. Effectively, stimulating transaction volume to a threshold of 25.4 transactions per block will slightly increase decentralization of decision-making power and improve the integrity of the blockchain.

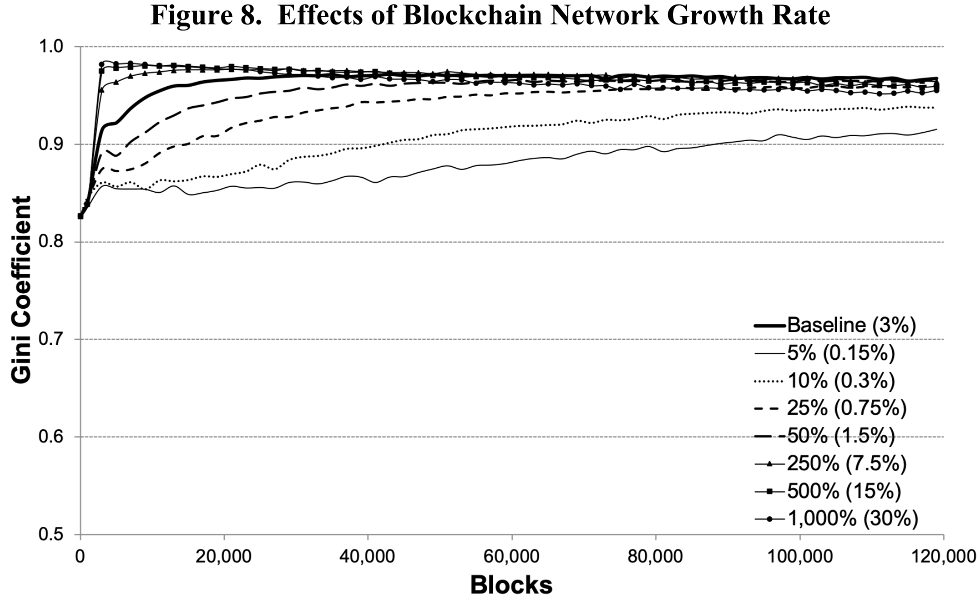
Figure 7. Effects of Transaction Volume



5.6. Blockchain Network Growth Rate

The final model parameter to be included in the sensitivity analysis concerns the growth rate of the blockchain network, that is, the rate at which new potential validator nodes join the network. The most substantial positive effect on decentralization is achieved by either very high or very low settings. While the low 5 and 10 percent settings produce the highest decentralization, these are followed by the 1,000 and 500 percent settings. This indicates that there is a nonlinear relation between blockchain network growth rate and decentralization of decision-making power, favoring either very low (0.15 - 0.3 percent) or high (15 - 30 percent) growth rates. In terms of its implications for blockchain governance, this result suggests that simply growing the blockchain network by adding high numbers of new nodes will have slightly adverse effects on the integrity of the blockchain. This can be mitigated only if blockchain operators ensure that new nodes entering the network possess a certain amount of currency stake to increase their chances of actually winning validations, rather than just absorbing currency and detracting from other nodes' chances at winning validations. If this is achieved, high growth rates may have a slight positive effect on decentralization of decision-making power.

Figure 8. Effects of Blockchain Network Growth Rate



5.7. Summary of Sensitivity Analysis Results

Overall, the sensitivity analysis identifies how changes in key blockchain parameters affect decentralization in PoS blockchains. Specifically, increases in the initial number of nodes, transaction amount, and transaction volume positively affect decentralization and thereby increase the integrity of the blockchain. Increases in transaction fees have a marginal negative effect on decentralization. The relationship between blockchain network growth rate and decentralization is non-linear, since very high and very low growth rates are associated with increased decentralization. The initial stake distribution does not affect decentralization, except for the highly skewed distribution, which is associated with a decreased level of decentralization. Table 5 provides statistical validation of the effects of model parameters on decentralization and Table 6 interprets these results for each model parameter.

Table 5. Regression Results

Variable	Coefficient	SE	*t*-value	*p*-value	Significance
Intercept	1.0309	0.0080	128.31	0.000	***
Bimodal	0.0003	0.0030	0.10	0.919	
Normal	0.0025	0.0030	0.82	0.411	
PowerLaw-1	0.0030	0.0030	0.96	0.337	
PowerLaw-2	0.0015	0.0030	0.48	0.635	
Skewed	0.0394	0.0030	12.77	0.000	***
Uniform	-0.0019	0.0030	-0.61	0.544	
$\ln(A_0)$	-0.0067	0.0006	-11.04	0.000	***
$\ln(F)$	0.0015	0.0006	2.49	0.013	*
$\ln(U)$	-0.0244	0.0006	-40.28	0.000	***
$\ln(V)$	-0.0082	0.0006	-13.52	0.000	***
$\ln(G)$	0.0451	0.0025	18.23	0.000	***
$\ln(G)^2$	-0.0052	0.0003	-18.05	0.000	***

$R^2 = 0.729$
Significance: *** $p<0.001$, ** $p<0.01$, * $p<0.05$
Notes: The dependent variable is the Gini coefficient, where higher values represent greater centralization and lower values represent greater decentralization. Therefore, coefficients that are negative are interpreted as increasing decentralization of decision-making power.

Table 6. Model Parameter Effects on Decentralization of Decision-Making Power

Model Parameter	Summary of Results
Design Parameters	
Initial stake distribution (*B*)	The decentralization of decision-making power is not affected by changes in initial stake distribution, except for stake distributions that are very highly skewed (e.g., one node possessing 90% of the total stake), in which case the centralization of decision-making power increases.
Initial number of nodes (A_0)	The decentralization of decision-making power increases with a higher number of potential validator nodes available at the genesis of the blockchain.
Transaction fee (*F*)	The decentralization of decision-making power decreases marginally with higher average transaction fees.
Behavioral Parameters	
Transaction amount (*U*)	The decentralization of decision-making power increases with larger average transaction amounts.
Transaction volume (*V*)	The decentralization of decision-making power increases with a higher average transaction volume per block.
Blockchain network growth rate (*G*)	The decentralization of decision-making power increases with either very high or very low blockchain network growth rates.

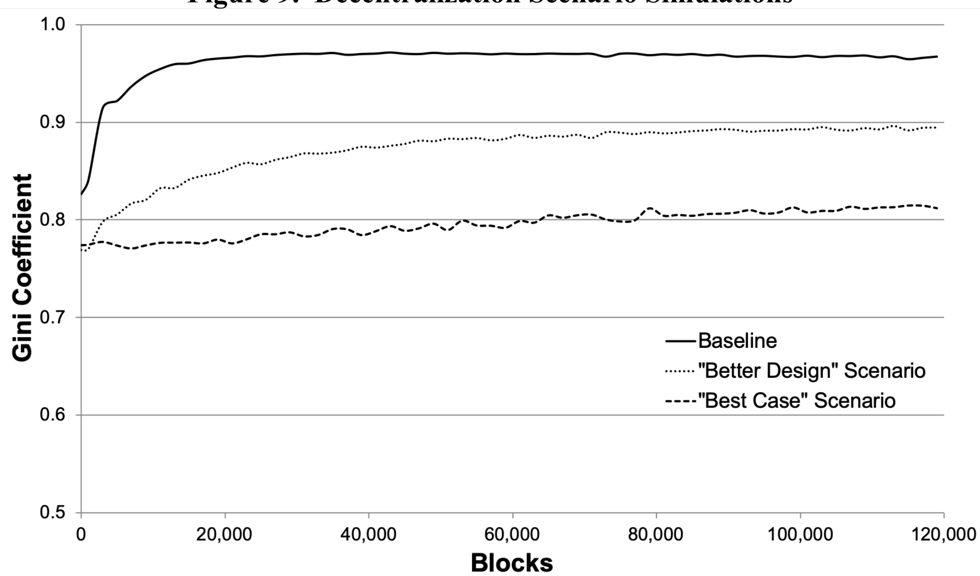
5.8. Further Scenario Testing

Having established the main effects of each of the model parameters, we can now explore various scenarios that can be expected to yield greater degrees of decentralization. First, we tested a "better design" scenario in which we only use design-related model parameters, that is, parameters that are directly accessible to manipulation in the design of blockchain systems. This is to explore how much decentralization might have been achievable by a PoS blockchain given its actual use context (i.e., in terms of transaction amounts, transaction volume and organic network growth rate) if the blockchain model parameters were set to levels that could achieve greater decentralization. Next, we move onto testing a "best-case" scenario by setting *all* model parameters (i.e., including the behavioral parameters) to settings that yielded positive effects on decentralization. This is to establish the conditions under which decentralization might best flourish and to estimate the extent of decentralization one might expect to achieve if the blockchain operator could also induce maximal decentralization producing behaviors (within the range of the parameter settings explored in the sensitivity analysis), such as setting the blockchain use context to one where average transactions amounts are very high (e.g., by setting the application domain to contexts such as financial settlements where average transaction amounts are high) and the network growth rate is contained (e.g., by controlling the entry of new nodes onto the network such as in permissioned blockchains).

The "better design" scenario uses settings for blockchain design parameters that yield the highest positive main effects on decentralization under the assumption that they will be mutually reinforcing (or at least not cancelling each other out) to produce a substantial increase in the degree of decentralization. More specifically, the design parameters (i.e., initial stake distribution, initial number of nodes, and average transaction fee) were set to maximally effective settings, but the behavioral parameters (i.e., transaction amount, transaction volume, and blockchain network growth) remained at levels that match the model baseline. Given the lack of impact of different initial stake distributions, apart from the skewed distribution which had an adverse effect, we set the initial stake distribution (B) as the model baseline; the initial number of nodes (A_0) was set to 730 at 1,000 percent of the model baseline; transaction fees (F) were kept at 5 percent of the baseline value equivalent to 21 NXT per transaction. While behavioral parameters such as transaction amount and volume might be stimulated through ongoing blockchain governance, they are outside the immediate scope of blockchain design. Given that the point of this exercise is to simulate the direct effects that design decisions might have on decentralization of decision-making power, the behavioral parameters were fixed at the model baseline. Specifically, average transaction amount (U) was set to 39,434 units of currency on average per transaction, transaction volume (V) to an average of 2.54 transactions per block, and the blockchain network growth rate (G) to a 0.03 (3 percent) increase in the number of nodes per block. Overall, as can be seen in Figure 9, optimizing the design parameters proved to produce a substantial improvement in overall decentralization (Gini ≈ 0.89) as compared to the model baseline (Gini ≈ 0.97).

Next, we explored the "best case" scenario where both design and behavioral parameters were set to maximally effective settings (within the bounds of the parameter settings used in the sensitivity analysis). We based the specific parameter values for the scenario on our results from the sensitivity analysis so that the initial stake distribution (*B*) was set at the baseline and initial number of nodes (A_0) was set to 730, or 1,000 percent of the model baseline of 73 initial nodes. This was the setting that produced the highest positive main effect, all else being equal. Similarly, the average transaction fee per block (*F*) was set to the lowest simulated setting at 21 units of currency, or 5 percent of the model baseline of 414 units of currency received by the validator node. Under the assumption that nodes with sufficient stake by default participate as potential validators, this might allow for more new potential validator nodes to stand a chance to win the right to validate and thereby lead to more decentralization. As transaction amount (in terms of the average currency amount in each transaction) displayed relatively large positive effects on decentralization of decision-making power, average transaction amount (*U*) was set to the maximum value of 394,340 units of currency at 1,000 percent of the model baseline. At an approximate value of USD 17,913 (using the median exchange rate for the first 120,000 blocks of the NXT blockchain), this is a very large amount to send on average across all transactions and therefore warrants consideration about the context in which the blockchain is implemented. With a large average transaction amount, transaction volume (*V*) must be kept at or near the model baseline—despite the fact that it shows some positive effect on decentralization—because a maximum setting for transaction volume in combination with large average transaction amounts comes too close to the market capitalization of the blockchain to be computationally feasible. We chose to simulate the maximum setting for transaction amount rather than transaction volume, since it shows a greater positive effect on decentralization of decision-making power. Given that the blockchain network growth rate has a negative effect on decentralization of decision-making power, we kept this parameter (G) at its lowest setting of 0.0015, or 5 percent of the model baseline at 0.03. Overall, the results show a profound effect in terms of increasing decentralization. As shown in Figure 9, the Gini coefficient for the "best case" scenario indicates a slight linear increase from approximately 0.78 to around 0.81, whereas the model baseline converges on a significantly higher value (Gini ≈ 0.97).

Figure 9. Decentralization Scenario Simulations



6. Discussion and Conclusion

Blockchain is a disruptive and transformational force, but the realization of its potential is highly contingent upon decentralization of decision-making power. Decentralization is critical for blockchain integrity and a key factor if blockchain is to fulfill its promise of removing trusted third parties. In this paper, we study how decision-making power in PoS blockchains becomes decentralized. We find that a high number of initial potential validator nodes, large transactions, and a high number of transactions increase the degree of decentralization. Our results also suggest that a very high or very low positive network growth rate increases the degree of decentralization. We only find weak support for an impact of changes in transaction fees and initial stake distributions on the degree of decentralization.

We contribute to the emerging literature on the PoS consensus mechanism. Roşu and Saleh (2021) find that for stable block rewards, the rich do not get richer. Our analysis confirms their results; our findings suggest that the degree of decentralization converges to a stable level with stable block rewards. Our study complements the study of Irresberger (2018), who focuses on the trade-off between coin inflation and decentralization, by studying PoS blockchains without inbuilt inflation. We also go beyond Irresberger (2018) in that we investigate the effects of changes in numerous key parameters on the degree of decentralization, instead of focusing on one specific trade-off. Overall, our findings contribute to a better understanding of the factors driving the decentralization of decision-making power in PoS blockchains, and can be applied to promote the decentralization of decision-making power, thereby making PoS blockchains less prone to attacks and more secure. In the following, we will discuss design implications of our study, as well as limitations and avenues for future research.

6.1. Design Implications

Our study provides implications for blockchain system design. With regard to the design parameters (i.e., initial stake distribution, initial number of nodes, and average transaction fee), we can derive several insights. To achieve high levels of decentralization, those setting up new PoS blockchain systems need to ensure the systems are initiated with a high number of potential validator nodes. To attract potential validator nodes before the launch of a blockchain systems, the initiators could advertise to relevant stakeholders and run a test network to allow interested stakeholders to familiarize themselves with the blockchain system. They could also offer financial rewards by selling stake at a discount to those willing to participate in transaction validation already from the system launch. Our findings also suggest that highly skewed initial stake distributions, in which a single person or group owns most of the stake, pose a centralization risk. In many cases, blockchain systems are initiated by a single individual or small group. Even though there may be an initial incentive for this person or group to retain most of the stake themselves, to ensure the long-term feasibility of the blockchain system, they should foster decentralization by selling off a significant portion of their stake before the blockchain launch. In line with prior research (Roşu and Saleh, 2021), we find that changes in transaction fees only have a marginal impact on the degree of decentralization. Therefore, design choices with respect to this parameter appear to not be critical for the decentralization of the blockchain system.

With regard to the behavioral parameters (i.e., transaction amount, transaction volume, and network growth), those setting up new PoS blockchain systems have only limited possibilities of manipulation. In particular, this is the case for transaction amount and transaction volume. On the other hand, blockchain network growth is to some extent available for manipulation. We find that high network growth will have slightly adverse effects on the degree of decentralization. To mitigate this, the blockchain initiators could increase the barriers to access for new nodes joining the network by setting up a permissioned blockchain. Such blockchains are characterized by restricted access for potential validators, and can virtually guarantee a certain degree of decentralization (Bakos et al., 2021). However, this is not feasible for PoS blockchain systems, since validation rights are tied to stake ownership, and stake can be acquired be anyone. Moreover, in many blockchain projects open access is highly desired, since a permissioned blockchain requires a central gatekeeper to grant access to transaction validation, which in turn introduces another centralization vulnerability. A more promising approach to curbing network growth may be to require nodes to own a large amount of stake to be eligible for validation. However, this would exclude less powerful nodes from having a chance to validate transactions, and may therefore also not be an option for many blockchain network designers, who often emphasize inclusivity.

6.2. Limitations and Future Research

Our research has a number of limitations representing important avenues for future research. First, our study focuses on analyzing the main effects of salient parameters in the blockchain, while interaction effects are not studied in detail. However, we analyzed interaction effects by conducting scenario testing, in which we manipulate several parameters at the same time to study the combined effects on the degree of decentralization. Our results suggest that both a "best-case" scenario, in which all parameters were set to yield a high degree of decentralization, and a "better design" scenario, in which all parameters which can be manipulated through design choices were set to yield a high degree of decentralization, are associated with substantial increases in decentralization. Even though our analysis does not suggest that the effects are cancelling each other out, future research could investigate these issues in more detail, discerning if there are interaction effects and whether their nature is reinforcing or balancing.

Second, our work only analyzes the PoS consensus mechanism. While we do believe that PoW with its energy expenditure may not be sustainable, less common variants of PoS have sprung up, such as delegated PoS, in which all nodes have voting rights (weighted by stake size) that they use to vote for a limited number of validator nodes. Our findings do not necessarily apply for such cases. However, PoS is the most common alternative to PoW, and indeed the most common consensus mechanism in newly launched blockchains (Irresberger et al., 2021). Since extant research mostly focuses on PoW, we believe more research on PoS is urgently needed; our paper contributes to addressing this research need. We also believe our work can be used as a guiding framework to study variants of PoS. The reason is that agent-based simulations could be used to study how blockchain systems based on consensus mechanisms such as delegated PoS become centralized or decentralized, depending on the node behavior and design choices. Another recently emerging type of stake-based voting is on-chain blockchain governance, where nodes can vote on governance proposals, such as changes to the consensus mechanism design itself (Tsoukalas & Falk, 2020). This phenomenon is also beyond the scope of our paper.

Third, our measure for the distribution of decision-making power in blockchains allows for only limited insights with respect to the concrete implications for blockchain integrity. Changes in the distribution of decision-making power can only reveal general tendencies in terms of their effects on blockchain integrity, yet we do not identify critical levels of centralization. Our conceptualization of the effect centralization of decision-making power has on blockchain integrity is, however, in line with the notion that the greater the relative decision-making power one node obtains, the more likely it is that its attack succeeds.

References

Alsabah, H., & Capponi, A. (2020). Pitfalls of bitcoin's proof-of-work: R&D arms race and mining centralization. Working paper, Columbia University.

Andersen, J. V., & Bogusz, C. I. (2019). Self-Organizing in Blockchain Infrastructures: Generativity Through Shifting Objectives and Forking. *Journal of the Association for Information Systems*, *20*(9), 1242-1273.

Arnosti, N., & Weinberg, S. M. (2019). Bitcoin: A natural oligopoly. *10th Innovations in Theoretical Computer Science, ITCS 2019* (p. 5). Schloss Dagstuhl-Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing.

Azouvi, S., Maller, M., & Meiklejohn, S. (2018). Egalitarian society or benevolent dictatorship: The state of cryptocurrency governance. In *International Conference on Financial Cryptography and Data Security* (pp. 127-143). Springer, Berlin, Heidelberg.

Bakos, Y., Halaburda, H., & Mueller-Bloch, C. (2021). When permissioned blockchains deliver more decentralization than permissionless. *Communications of the ACM*, *64*(2), 20-22.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the age of blockchains. Working paper, University College London and The Alan Turing Institute.

Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, *19*(10), 1020-1034.

Benetton, M., Compiani, G., & Morse, A. (2021). When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy. Working paper, University of California.

Biais, B., Bisière, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies, 32*(5), 1662–1715.

Bloomfield, B. P., & Coombs, R. (1992). Information technology, control and power: The centralization and decentralization debate revisited. *Journal of Management Studies*, *29*(4), 459-484.

Bonabeau, E. (2002). Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences, 99*(suppl. 3), 7280-7287.

Bonneau, J. (2018). Hostile blockchain takeovers (short paper). *International Conference on Financial Cryptography and Data Security* (pp. 92-100). Springer.

Carlsten, M., Kalodner, H., Weinberg, S. M., & Narayanan, A. (2016). On the instability of bitcoin without the block reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 154-167).

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Communications of the ACM, 63*(7), 80-90.

Cennamo, C., Marchesi, C., & Meyer, T. (2020). Two sides of the same coin? Decentralized versus proprietary blockchains and the performance of digital currencies. *Academy of Management Discoveries*, *6*(3), 382-405.

Clemons, E. K., Dewan, R. M., Kauffman, R. J., & Weber, T. A. (2017). Understanding the information-based transformation of strategy and society. *Journal of Management Information Systems, 34*(2), 425-456.

Cong, L. W., He, Z., & Li, J. (2021). Decentralized mining in centralized pools. *The Review of Financial Studies, 34*(3), 1191-1235.

Constantinides, P., Henfridsson, O., & Parker, G. (2018). Introduction—Platforms and Infrastructures in the Digital Age. *Information Systems Research*, *29*(2), 381-400.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys & Tutorials*, *20*(4), 3416-3452.

Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In *IEEE P2P 2013 Proceedings* (pp. 1-10). IEEE.

Drazin, R., & Sandelands, L. (1992). Autogenesis: A perspective on the process of organizing. *Organization Science, 3*(2), 230-249.

Ein-Dor, P., & Segev, E. (1978). Centralization, decentralization and management information systems. *Information & Management*, *1*(3), 169-172.

Epstein, J. M. (2006). *Generative social science: Studies in agent-based computational modelling*. Princeton University Press.

Gastwirth, J. L. (1972). The Estimation of the Lorenz Curve and Gini Index. *The Review of Economics and Statistics*, *54*(3), 306-16.

Gell-Mann, M. (1994). Complex adaptive systems. In G. Cowan, D. Pines, & D. Meltzer,(Eds.), *Complexity: Metaphors, Models, and Reality* (pp. 17-29). Addison-Wesley.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3-16).

Haki, K., Beese, J., Aier, S., & Winter, R. (2020). The Evolution of Information Systems Architecture: An Agent-Based Simulation Model. *MIS Quarterly*, *44*(1), 155-184.

Halaburda, H., & Mueller-Bloch, C. (2020). Toward a Multidimensional Conceptualization of Decentralization in Blockchain Governance: Commentary on "Two Sides of the Same Coin? Decentralized versus Proprietary Blockchains and the Performance of Digital Currencies" by Cennamo, Marchesi, and Meyer. *Academy of Management Discoveries, 6*(4), 712-714.

Holland, J. H. (1992). *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence*. MIT Press.

Holland, J. H. (1995). *Hidden Order: How Adaptation Builds Complexity*. Addison-Wesley.

Hsieh, Y. Y., Vergne, J. P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin and the rise of decentralized autonomous organizations. *Journal of Organization Design*, *7*(1), 1-16.

Irresberger, F. (2018). Coin concentration of proof-of-stake blockchains. Working paper, Durham University.

Irresberger, F., John, K., & Saleh, F. (2021). The public blockchain ecosystem: An empirical analysis. Working paper, New York University Stern.

King, J. L. (1983). Centralized versus decentralized computing: Organizational considerations and management options. *ACM Computing Surveys (CSUR)*, *15*(4), 319-349.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*(1).

Klügl, F. (2008). A validation methodology for agent-based simulations. In *Proceedings of the 2008 ACM Symposium on Applied Computing* (pp. 39-43).

Kroll, J. A., Davey, I. C., & Felten, E. W. (2013). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In *Proceedings of the Twelfth Workshop on the Economics of Information Security.*

Lerman, R. I., & Yitzhaki, S. (1984). A note on the calculation and interpretation of the Gini index. *Economic Letters, 15*(3-4), 363-368.

Litchfield, J. A. (1999). Inequality: Methods and tools. World Bank, available at: https://siteresources.worldbank.org/INTPGI/Resources/Inequality/litchfie.pdf

Lumineau, F., Wang, W., & Schilke, O. (2021). Blockchain governance—A new way of organizing collaborations?. *Organization Science*, *32*(2), 500-521.

Markus, M. L., & Bjørn-Andersen, N. (1987). Power over users: its exercise by system professionals. *Communications of the ACM*, *30*(6), 498-504.

Miller, J. H., & Page, S. E. (2009). *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*. Princeton University Press.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. White paper, available at https://bitcoin.org/bitcoin.pdf.

Nan, N. (2011). Capturing bottom-up information technology use processes: A complex adaptive systems model. *MIS Quarterly, 35*(2), 505–532.
Nan, N., & Tanriverdi, H. (2017). Unifying the role of IT in hyperturbulence and competitive advantage via a multilevel perspective of IS strategy. *MIS Quarterly, 41*(3), 937-958.
Peters, D. H. (2014). The application of systems thinking in health: Why use systems thinking? *Health Research Policy and Systems, 12*(1), 1–6.
Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering*, *59*(6), 385-409.
Rivkin, J. W., & Siggelkow, N. (2007). Patterned interactions in complex systems: Implications for exploration. *Management Science, 53*(7), 1068-1085.
Rossi, M., Mueller-Bloch, C., Thatcher, J. B., & Beck, R. (2019). Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda. *Journal of the Association for Information Systems*, *20*(09), 1390-1405.
Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. *Information Processing & Management*, *58*(4), 102584.
Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of Financial Studies, 34*(3), 1156-1190.
Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: a theory of multiple contingencies. *MIS Quarterly*, *23*(2), 261-290.
Schelling, T. C. (1969). Models of segregation. *American Economic Review, 59*(2), 488–493.
Shanaev, S., Shuraeva, A., Vasenin, M., & Kuznetsov, M. (2019). Cryptocurrency value and 51% attacks: evidence from event studies. *The Journal of Alternative Investments, 22*(3), 65-77.
Siggelkow, N., & Levinthal, D. A. (2003). Temporarily divide to conquer: Centralized, decentralized, and reintegrated organizational approaches to exploration and adaptation. *Organization Science, 14*(6), 650-669.
Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Research commentary—Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, *21*(4), 675-687.
Tschorsch F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials, 18*(3), 2084–2123.
Tsoukalas, G., & Falk, B. H. (2020). Token-weighted crowdsourcing. *Management Science, 66*(9), 3843-3859.
Vergne, J. P. (2020). Decentralized vs. distributed organization: blockchain, machine learning and the future of the digital platform. *Organization Theory*, *1*(4), 1-26.
Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press.
World Bank Institute (2005). Introduction to Poverty Analysis, available at http://siteresources.worldbank.org/PGLP/Resources/PovertyManual.pdf
Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and Organization*, *29*(2), 105-117.

Zhang, J., Adomavicius, G., Gupta, A., & Ketter, W. (2020). Consumption and performance: Understanding longitudinal dynamics of recommender systems via an agent-based simulation framework. *Information Systems Research*, *31*(1), 76-101.

APPENDIX A. MODEL PSEUDO CODE

```
INPUT:
\\ All input multipliers vary from 0.05 to 100 and are applied to the 5 parameters.

        initial_validator_multiplier
        fee_multiplier,
        send_amount_multiplier,
        transactions_per_block_multiplier,
        current_validator_count_multiplier

CONSTANTS:
\\ All constants are variables that do not change throughout the simulation

        total_stake \\ total stake that exists in the blockchain

GLOBAL VARIABLES:
\\ Global variables are updated throughout the simulation and help maintain the state of the
blockchain.

        current_block \\ current state of the blockchain
        timestamp = 0 \\ time in seconds since the first block
        previous_timestamp = the timestamp taken from the previous block


Function simulate_blockchain(input)
\\ This runs the simulation using the classes and functions defined

        simulation_model = new Model(input) \\ creates an instantiation of the model class
        FOR i in 1 to 120000
                simulation_mode.model_step() \\ calls the model_step function for each block
        ENDFOR

class Model(initial_validator_multiplier, fee_multiplier, send_amount_multiplier,
            transactions_per_block_multiplier, current_validator_count_multiplier)

        previous_generation_signature = DEFAULT NXT VALUE
        base_target = DEFAULT NXT VALUE
        previous_base_target = DEFAULT NXT VALUE
        Initial_validator_count = DEFAULT NXT VALUE * initial_validator_multiplier
        average_fee = DEFAULT NXT VALUE * fee_multiplier
        average_send_amount = DEFAULT NXT VALUE * send_amount_multiplier
        average_transactions_per_block = DEFAULT NXT VALUE * transactions_per_block_multiplier
        needed_validator_count= current block * current_validator_count_multiplier
        agent_validator_list = [ ]

        FOR 1 to initial_validator_count
                agent_validator_list.append(new Agent(total_stake / initial_validator_count))
        ENDFOR

        Function model_step()
        \\ Each step in the model simulates a single block in the blockchain

                FOR each Agent in agent_validator_list
                        Agent.agent_step() \\ Calls the agent_step function of each agent
                ENDFOR

                create_transactions()
                validate_block(current_block) \\ Rewards the agent with the highest decision-
                making power
                current_block += 1 \\ Increments the counter variable of the current block

        Function create_transactions()
        \\ Creates all transactions for current block
```

```
        FOR each transaction in average_transactions_per_block
            create_transaction(average_fee, average_send_amount)
            \\ Stake is redistributed by creating a transaction where the
            sender/recipient is   randomly selected unless the needed_validator_count
            does not match, in which the transaction will go to a new user
        ENDFOR

Class Agent(initial_stake)
\\ Each agent simulates a validator in the blockchain

    stake = initial_stake
    public_key \\ A unique identifier for this agent
    generation_signature \\ A hash of the previous generation signature and public_key
    hit \\ each agent has a unique hit which is highly random integer
    decision_power = 1000000.0 / hit / stake
    hit_time = hit / stake

    Function agent_step()
    \\ Recalculate the hit in order to recalculate the decision-making power of an individual
    agent

        hit = calculate the hit using the previous generation signature and the agent
        public_key
        target = stake * base_target
        hit_time = hit / target
        decision_power = 1000000.0 / hit / target
```