3
Deconstructing “Decentralization”
Exploring the Core Claim of Crypto Systems

Angela Walch[*]

> *Decentralization is what allows Bitcoin to substitute an army of computers for an army of accountants, investigators, and lawyers.*
>
> —Nick Szabo, Twitter.[1]

> *[B]ased on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions . . .*
>
> —William Hinman, Director, Division of Corporation Finance, SEC, Remarks at the Yahoo Finance All Markets Summit: Crypto: Digital Asset Transactions: When Howey Met Gary (Plastic).[2]

> *I’m a little worried people from government agencies are throwing around the word “decentralization” like we know what it means and how to evaluate it.*
>
> —Neha Narula, Director, MIT Digital Currency Initiative, Twitter.[3]

> *So I spent a couple weeks reading everything I could about the term “decentralization” and have come to a conclusion: we should ditch the term.*
>
> —Tony Sheng, *Let’s ditch “decentralized,”* www.tonysheng.com.[4]

[*] Professor of Law, St. Mary’s University School of Law. Research Fellow, Centre for Blockchain Technologies, University College London. I would like to thank Edmund Schuster, Peter Van Valkenburgh, Nic Carter, Oliver Beige, Ciaran Murray, Michèle Finck, Michel Rauchs, Gina Pieters, Stefan Loesch, Frances Coppola, Carla Reyes, Kristin Johnson, Usha Rodrigues, Joan Heminway, Odysseas Sclavounis, Andrew Glidden, Paolo Saguato, Chris Brummer, Drew Hinkes, Stephen Palley, Nelson Rosario, Brett Scott, Vlad Zamfir, participants at Fintech Week 2018 at the Institute for International Economic Law at Georgetown Law School on Nov. 5–8, 2018; participants in the Cryptoassets and the Law Workshop at the London School of Economics on Sept. 4, 2018; participants at the 4th Annual Law & Money Conference at Sheffield Law School on Sept. 3, 2018; participants in the Securities Law section discussion at the Association of American Law Schools 2019 Annual Meeting on Jan. 5, 2019; students in my Fall 2018 Blockchain Technologies, Cryptocurrencies & the Law course; and the active crypto Twitterverse for valuable discussions, feedback, and insights. I thank Rebecca Bredt for excellent research assistance.

Cryptoassets. Chris Brummer.
© Oxford University Press 2019. Published 2019 by Oxford University Press.

On June 14, 2018, William Hinman, Director of the SEC's Division of Corporation Finance, seized the crypto[5] world's attention when he stated that "current offers and sales of Ether are not securities transactions" and linked this conclusion to the "sufficiently decentralized" structure of the Ethereum network.[6]

While one speech of an SEC employee does not binding law make, Hinman's was notable in demonstrating how pervasive the belief that blockchains are "decentralized" has become, and that a blockchain's level of "decentralization" is being used to draw conclusions—and potentially make legal decisions—about these systems.

If this is the case, and "decentralized" is transitioning from a marketing term for cryptoassets to one of legal import, we must be clear about what we mean when we describe blockchain networks or systems as "decentralized."[7] Do we mean they have lots of computer nodes running the software, and that those nodes are distributed across the globe? That the software development process is spread amongst many developers who have similar authority to make changes to the software? That the hashing power of record producers (miners) in the network is not concentrated in a small group?

This chapter does not provide a securities law analysis of Ethereum or any other blockchain system, as it has broader goals. Gaining a deeper understanding of the concept of "decentralization" in blockchain systems is important even if the SEC and the courts decide not to make a blockchain's level of decentralization relevant to a cryptoasset's status as a security.[8] This is because the term "decentralized" is generally being used to describe how power operates in blockchain systems—suggesting that power exercised by people in these systems is diffuse rather than concentrated. This is critically important, as our understanding of how power is exercised within these systems will shape conclusions about how responsibility, accountability, and risk should work for them—that is, pretty much every legal determination we make about them. So, it's simply not good enough to say that a blockchain system is decentralized because, well, blockchains are decentralized, and this is a blockchain. We must decide whether "decentralized" is a meaningful way to evaluate a blockchain system, and if so, we must be precise about what we mean by the term, and which portions of a complex blockchain system we are referring to. The concept of "decentralization" is a foundational, infrastructural one for blockchains—if we gloss over what it means, we risk unintended consequences when these systems do not behave like we expect them to.[9]

In this chapter, I seek to do several things. In Section I, I describe the current use of the term "decentralized" as applied to permissionless blockchains like Bitcoin and Ethereum,[10] and argue that the term has been widely used to suggest that these systems are resilient and that there is a lack of centralized (and therefore accountable) power wielded in these systems. In Section II, I analyze the complex, contested nature of the term, delving into issues such as the different domains where power is exercised in blockchain systems and the fluid nature of power concentration and diffusion in these systems. In Section III, I provide examples of events that reveal sites of concentrated power in permissionless blockchain systems, focusing on the activities of software developers and miners. Finally, in Section IV, I explore the significant implications for law of using a fuzzy term such as "decentralized" to make legal decisions, as misunderstandings about power hidden in the term can lead to flawed decisions across a wide swath of legal fields. I conclude that making decisions based on an unsubstantiated conclusion that a given blockchain (or blockchains generally) is (are) "decentralized" is highly problematic, and that courts, regulators, and even potential adopters or users of cryptoassets (whether directly or through other financial products) should use other factors to inform their decisions about a blockchain. Like many other descriptors of blockchain technology (e.g., immutable, trustless, reflects truth), the adjective "decentralized" as an inevitable characteristic of blockchain technology proves to be an overstatement, and we know that making decisions based on overstatements rather than reality can lead to bad consequences.[11]

I. Mainstream Discourse around "Decentralized" Permissionless Blockchains

Virtually every description of cryptoassets or blockchain technologies includes the adjective "decentralized."[12] Indeed, "decentralization" is viewed as a core feature of blockchain systems, and one of the magic ingredients that is said to enable these systems to generate a record that is very difficult to alter, reliably reflects transactions in the system's native digital token,[13] and does not require trust in a single, central party.

In this Section I, I discuss the mainstream use of the term "decentralized" in blockchain systems, and argue that the term is often used to suggest that blockchain systems are (1) resilient, and (2) free from the exercise of concentrated power. As we will see, this includes Director Hinman's comments about how the decentralization of a blockchain system relates to its token's status as a security.

First, it is important to emphasize how ubiquitous the terms "decentralized" and "decentralization" are in the discourse around blockchain technologies and cryptoassets.[14] The terms are present in academic works of relevant disciplines,[15] in discussions within the crypto space, in conference names galore,[16] and in countless reports by businesses, governments and international organizations. Software applications built on top of the Ethereum blockchain are known as "dapps"—short for "decentralized applications." There are multiple "decentralized exchanges" (known as "DEXs" in the industry) being built, which seek to break up the power that centralized exchanges such as Coinbase and Binance have accrued in the sector.[17] Legislators are using these words in statutory definitions of blockchain technology.[18] In short, the words "decentralized" and "decentralization" are inescapable in discussions about the technology.

Further, in mainstream discourse, it has been rare to see clear explanations of "decentralized" or "decentralization" when they are used. For example, in Arizona's statute that uses the term "decentralized" to define "blockchain technology," there is no definition of "decentralized" to be found.[19] Most mainstream descriptions of blockchain technologies or cryptoassets state simply that blockchains are decentralized. End of story. Decentralized is just something that blockchains are. An inherent characteristic. An essential and identifying feature. As I will discuss in Section II, this reflexive use of "decentralized" contrasts sharply with an active discussion among academics and thought leaders within the crypto space about the problematic nature of the term.

"Decentralized" is used in several senses in mainstream blockchain discourse. First, it is used to describe the network of computers (often referred to as "nodes") that comprise a permissionless blockchain, as these systems operate through peer-to-peer connections between computers, rather than on a central server. A core feature of permissionless blockchains such as Bitcoin or Ethereum is that the record generated by the system is stored on many computers within the network, rather than just on one. The idea is that many of the nodes are independent, so that a failure of one does not mean a failure of many or all. This "decentralized" storage of the record supports claims that the record is highly resilient, as the record is likely to persist so long as at least one of the computers continues to hold it. Of course, many factors could influence the actual resilience of the network, such as the geographical distribution of the nodes (affecting their common vulnerability to weather, natural disasters, and the like) or the common ownership of them (one party may own many and could turn all of its nodes off at once). But, at base, because there is not a central computer maintaining the blockchain record, it is *decentralized* rather than *centralized* (more than one party is involved).

The second way "decentralized" is commonly used is to describe how power or agency works within permissionless blockchain systems.[20] If there is not a single, central party keeping the record, that means that no single party has responsibility for it, and thus no single party is accountable for it. This concept of decentralization, or power diffusion, has more political or ideological undertones to it, and seems tied to the cypher-punk, crypto-anarchist roots of Bitcoin (the first blockchain). In serving as a money outside of state control, Bitcoin was a reaction to the central power of a state, and if those who were part of the system could convince the public (as well as the state) that power was diffuse within the system, then no particular person could be held legally accountable for what happened in connection with the system. In a "decentralized" system like Bitcoin, one could convincingly argue that power was everywhere and nowhere at the same time, that, in Melanie Swan's words, "authority float[s] freely."[21] Those in the permissionless blockchain world talk about seizing power from the state and existing powerful institutions like banks or tech platforms (e.g., Google or Facebook), and building a new "decentralized world," where power has been spread around.[22] Within the crypto space, Bitcoin advocates often criticize other permissionless blockchains as not truly decentralized, pointing to clusters of power or agency within the systems. To be fully decentralized (whatever that means) is viewed as one of the ultimate goals of a permissionless blockchain system, a utopian summit to be scaled.[23]

In picking up the terms from the crypto space, and using them uncritically (or at least with insufficient critical inquiry), the conflations and overstatements embedded in the terms have helped to establish people's beliefs about the characteristics of permissionless blockchain systems. As I argued in an earlier paper, the terminology in the blockchain space is highly problematic and misleading, due to numerous factors.[24] As I will discuss further in Section II, decentralization is inherently both a political concept and a physical description of computer networks. Here, both political (no one has any power, especially not the state) and physical (we have a lot of computers running, so you can't easily knock the entire system out) meanings have melded in mainstream usage of the terms.

Perhaps unsurprisingly, Director Hinman's June 2018 speech reflected these melded meanings of "decentralized," and thus seems representative of the common narrative around decentralization in permissionless blockchains. Here are relevant excerpts from the speech.

> If the network on which the token or coin is to function is sufficiently decentralized—where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts—the assets may not represent an investment contract. . . .
>
> [W]hen the efforts of the third party are no longer a key factor for determining the enterprise's success, material information asymmetries recede. As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful. . . .

> [W]hen I look at Bitcoin today, I do not see a central third party whose efforts are a key determining factor in the enterprise. The network on which Bitcoin functions is operational and appears to have been decentralized for some time, perhaps from inception. . . .
>
> [B]ased on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions. . . .
>
> Over time, there may be other sufficiently decentralized networks and systems where regulating the tokens or coins that function on them as securities may not be required. And of course there will continue to be systems that rely on central actors whose efforts are a key to the success of the enterprise.[25]

In these excerpts, we see an emphasis on (1) networks and (2) difficulty in identifying or "seeing" a central party playing a determining role in the system. In each of these excerpts, "decentralized" is used to describe the *network* of the applicable blockchain (Bitcoin or Ethereum) (e.g., "if the *network* . . . is sufficiently *decentralized*," "as a *network* becomes truly *decentralized*," "[t]he *network* on which Bitcoin functions . . . appears to have been *decentralized* for some time," "based on my understanding of the present state of Ether, the Ethereum *network* and its *decentralized* structure," and "there may be other sufficiently *decentralized networks* and systems"). This phrasing suggests that Hinman is looking at the network of computers that comprise the Ethereum and Bitcoin systems to support his statements that the systems are decentralized—that is, using the physical connotation of "decentralized."

Further, we see in these excerpts statements that it is difficult to find a central party within the systems who is determining what happens in the system (e.g., "[a]s a network becomes truly decentralized, the ability *to identify* an issuer or promoter to make the requisite disclosures becomes difficult . . . ," "when I look at Bitcoin today, I *do not see* a central third party whose efforts are a key determining factor in the enterprise"). The language here is suggestive of vision or sight—Hinman *cannot see* a central third party doing important things in systems such as Bitcoin or present-day Ethereum to ensure the systems' success.

Why is Hinman focusing on the ability to identify a party who could make required disclosures about the token of a blockchain system? Because it is relevant to determining whether an instrument (here, a blockchain token) is a security under the U.S. securities laws.[26] Hinman uses the concept of decentralization to refer to how people exercise power within the Bitcoin and Ethereum systems, consistent with my claim about mainstream usage of the term "decentralized." (Interestingly, he appears to be conflating the physical features of the network (which impact its resilience) with the way power works within the system.) The standard for determining whether a transaction represents an "investment contract" and thereby a security comes from the venerable *SEC v. W.J. Howey Co.*, a 1946 U.S. Supreme Court case about interests in citrus groves.[27] The *Howey* test states that there is an investment contract (and thereby a security) when there is (1) a contract, transaction, or scheme; (2) whereby a person invests money; (3) in a common enterprise; and (4) is led to expect profits solely from the efforts of others.[28] The fourth factor has been expanded over the years to remove the requirement that profits be expected *solely* from the efforts of others. Hinman indicates whose efforts would be relevant in his June 2018 remarks:

> *The important factor in the legal analysis is that there is a person or coordinated group (including "any unincorporated organization" see 5 U.S.C. § 77n(a)(4)) that is working actively to develop or guide the development of the infrastructure of the network.* This person or group could be founders, sponsors, developers or "promoters" in the traditional sense. The presence of promoters in this context is important to distinguish from the circumstance where multiple, independent actors work on the network but no individual actor's or coordinated group of actors' efforts are essential efforts that affect the failure or success of the enterprise.[29]

Hinman also provides a series of questions to guide potential token issuers as to whether their token offering will be considered a securities offering. Several of the questions focus on power exercised by people within the blockchain system, that is, "whether a third party—be it a person, entity or coordinated group of actors—drives the expectation of a return [from the sale of the token]."[30] These questions include:

(1) Is there a person or group that has sponsored or promoted the creation and sale of the digital asset, the efforts of whom play a significant role in the development and maintenance of the asset and its potential increase in value?
(2) Does application of the Securities Act protections make sense? Is there a person or entity others are relying on that plays a key role in the profit-making of the enterprise such that disclosure of their activities and plans would be important to investors? Do informational asymmetries exist between the promoters and potential purchasers/investors in the digital asset?
(3) Do persons or entities other than the promoter exercise governance rights or meaningful influence?[31]

The excerpted portions of Hinman's speech all suggest that the term "decentralized" is being used to describe how power works in a given blockchain system—whether certain actors' actions "are essential efforts that affect the failure or success of the enterprise."[32] Hinman's statement that both the Bitcoin and Ethereum blockchain systems are "sufficiently decentralized" such that their tokens are not securities indicates that, according to his understanding of Bitcoin and Ethereum as of June 14, 2018, neither system contained "a person or coordinated group (including "any unincorporated organization" . . .) that [wa]s working actively to develop or guide the development of the infrastructure of the network."[33] Again, using Hinman's language, he "*do[es] not see* a central third party whose efforts are a key determining factor in the enterprise."[34]

It is unsurprising, therefore, that industry organizations for the crypto and blockchain sector have strongly endorsed Hinman's use of "decentralization" to help to determine whether a blockchain token is a security.[35] The newly formed Blockchain Association, an industry trade organization, has called for "decentralization" to be measured under "The Hinman Token Standard," arguing that the characteristics that both Ethereum and Bitcoin possessed on the day of Hinman's speech (June 14, 2018) should set a ceiling on the requirements for a system to be "sufficiently decentralized" that its token is not a security.[36] The Blockchain Association stated:

> [D]evelopers of open source, public blockchain networks and those in the community that help foster their development should work with counsel to understand that the announced Hinman Token Standard likely *has not set an impossibly or unreasonably high standard for decentralization*. Open-source and cryptocurrency projects often need or choose to have *some* centralized leadership, and at times considerable centralized leadership on their path to decentralization. As demonstrated by both bitcoin and ether, the Hinman guidance has established that having some level of centralized leadership will not condemn a token to being classified as a security on that basis alone.[37]

Tellingly, the Blockchain Association acknowledges the "centralized leadership" present in both Bitcoin and Ethereum, which does support its argument that the SEC has set a low bar to be considered "sufficiently decentralized." I agree with the trade group that the SEC's standard for "sufficiently decentralized" is extremely low,[38] and seek to demonstrate in Sections II and III of this chapter that a deeper analysis of the concept is needed.

* * *

In this Section I, I have painted a picture of the ways "decentralized" is used in common discourse, focusing on the common use of the term within the academic, governmental, and industry domains, and particularly on SEC

Director Hinman's use of the term to support his statement that Bitcoin and Ether are not securities. I argue that the term is used (1) to describe the network features (e.g., number of computers in the network), supporting claims that a blockchain system is resilient; and (2) to describe how power operates in the system, supporting claims that power is diffuse and must therefore be unaccountable. I see both of these common meanings as imprecise, and potentially completely inaccurate (depending on which blockchain system we're talking about), and in Section II, I delve deeper into the meaning of "decentralized" as applied to blockchain systems.

II. The Complex Nature of "Decentralization"

In this section, I analyze the concept of decentralization in permissionless blockchains, in order to demonstrate the complex, contested meaning of the term. It turns out I am far from alone in critiquing the use of "decentralized" to describe blockchain systems. In fact, in the past few years, exploring the concept of "decentralization" has become a trend for thought leaders and academics in the crypto space.[39] Venture capitalists, Ethereum creator Vitalik Buterin, and others have attempted to articulate what "decentralization" means.[40] In this subsection, I provide an overview of these takes, drawing out the important themes. This analysis will buttress my arguments in Section IV about the implications of making legal decisions based on a superficial conclusion that a given permissionless blockchain system is decentralized.

Notable Themes

A. No One Knows What "Decentralization" Means

A pervasive theme of all analyses is that decentralization is often discussed as essential and a feature that differentiates crypto systems from others, yet it is much more complex than commonly realized, and is poorly understood.

Part of the complexity in the concept stems from the complexity of permissionless blockchain systems themselves. Crypto systems are comprised of many different actors, including the developers who write and maintain the software code, the miners (or record producers) who process transactions and add them to the common record, and the nodes, who send transaction to miners and maintain copies of the blockchain record. Many commentators noted that the decentralization level of a crypto system as a whole was dependent upon each subsystem within it being decentralized as well.[41] So, for example, if the software development process is centralized to a small number of developers, the system as a whole could not be considered decentralized, even if mining was widely distributed and there were thousands of nodes spread throughout the globe. Some noted that actors outside the system could also impact the decentralization level of a crypto system. Exchanges were noted as a site of potential centralization, as they have the power to choose whether or not to list a particular token for trading.[42] Holders of tokens were cited by others as potential sites of centralization, as in many crypto systems, ownership is concentrated in a very small number of people (often referred to as "whales"). The number of software implementations of a blockchain system's protocol could also affect centralization, particularly if there is a dominant one.[43] Thus, it is not helpful to describe a blockchain system as decentralized unless one is specific about how he or she is measuring the level of decentralization in each domain of the system.

A number of analyses noted that attempts at quantification of decentralization were more meaningful in certain subsystems than in others. For instance, it is possible to count numbers of computer nodes within a system, and potentially (though not very easily, probably) determine how ownership of the nodes is distributed. Similarly, one could measure percentages of hashing power held by a given miner or mining pool.[44] These domains lend themselves to numeric measurements. Yet, as emphasized by commentators such as Sarah Jamie Lewis, Nic Carter, and Michel Rauchs et al., the governance of the software development process is just as relevant to how decentralized a system is, but is much more difficult to quantify or measure, as it deals with the behavior of individuals and often unwritten norms.[45] Moreover, behind every computer in the network, whether miner or node, there is ultimately a person who controls the computer, whose human unpredictability may bleed into governance of the system in unexpected ways.

B. Satoshi Didn't Invent Decentralization

Although "decentralize all the things" has become something of a rallying cry in the crypto world, commentators noted that the concept of decentralization has a long history, both inside and outside the realm of technology. Finck and Barabas et al. link the current excitement about disrupting large institutions through decentralization to that of the early days of the internet.[46] Carter notes the relevance of political science and sociology literature on decentralized governance, as well as the history of open-source software governance.[47] Atzori's excellent political analysis of blockchain-based decentralized governance explores where it is situated in various strands of political theory.[48]

The political or ideological roots of the concept of decentralization is, unsurprisingly, a common theme. Decentralization is fundamentally about diffusing power by distributing it away from a central point of control—sharing that power among many. The idea of decentralization is, of course, a foundational principle of many of our most basic institutional governance structures, from the federalist system that shares power between the states and federal government in the United States, to the checks and balances inherent in the three branches of the U.S. government, to the principle of subsidiarity in the European Union that pushes power away from the center. Decentralization is often about disruption or revolution—breaking up existing power structures, with hopes of spreading power around. The decentralization mantra around blockchains follows in that vein, including the discussions about "being your own bank" or "owning your digital identity" or creating money not issued by a central bank.

C. Decentralized Does Not Equal Distributed

The terms "distributed" and "decentralized" are often used interchangeably in describing blockchain systems. According to the Cambridge Centre for Alternative Finance's *Distributed Ledger Technology Systems: A Conceptual Framework* (the "CCAF Report"), "decentralized" is used to indicate that the nodes operating in a system are controlled by different parties, rather than by the same entity.[49] The CCAF Report states that "distributed" is used to indicate that "storage or computation . . . is divided into parts and occurs across multiple servers or nodes ("parallelized"), but "may still rely on a central coordinator to act as an authoritative source of records."[50]

D. Decentralization Exists on a Spectrum

The CCAF Report points out that "decentralization" of a distributed ledger technology system (including a permissionless blockchain) "is not a simple binary property," as "the degree of centralization reflects the accumulation of interacting decisions and tradeoffs at various layers. In practice, it is more useful to identify the contributing factors to centralization and decentralization across a spectrum, as pure decentralization is a seldom-achieved ideal at both the hardware and software levels."[51] Indeed, it is helpful to envision a spectrum of centralization, with any change made to a given subsystem (e.g., nodes, developers, miners) moving the system toward greater or lesser centralization, rather than a bright line demarcating centralized versus decentralized.

E. Decentralization Is Dynamic rather than Static

The CCAF Report notes that the "power dynamics" within a blockchain system "can be fluid and evolve over time, which further complicates the task of forming a definitive assessment of the system."[52] Hinman's speech also hints at the dynamic nature of decentralization by stressing that his conclusions about whether Ether is a security are based on its characteristics (i.e., its level of decentralization) as of the date of his speech.

The fluctuating nature of a system's level of decentralization is worth emphasizing, as every passing second could bring massive changes to it. So many factors affect how decentralized a blockchain system is that a change to *any* of those factors can shift the blockchain on the decentralization spectrum. For instance, if a significant miner loses power due to a natural disaster or is shut down by a government, the power dynamics within the mining network will shift. If one of the core developers who has the password to merge changes to a particular blockchain software client loses this privilege because the other core developers no longer trust him, the power dynamics within the software development process will shift. If it becomes prohibitively expensive to run a node, or a rumor circulates that running a node is illegal and many nodes drop out, that will shift the level of decentralization of the system.

The critical takeaway here is that any measurement of decentralization is obsolete immediately after it has been calculated. In a permissionless system, anyone can join, and no one has to stay, so the system's composition is, in theory, always in flux.

F. Decentralization Is Aspirational, Not Actual

Commentators have noted that "decentralization" in blockchain systems is not something that has been achieved yet, but instead is merely a goal of current systems.[53] This emphasizes how immature the development of blockchain technologies is, as well as the limited progress that has been made in building a "decentralized world." Another way of putting it is that at present, decentralization in blockchain systems is "all hat, no cattle."

Some initiatives are open about their current, highly concentrated power structures, noting that they need centralized decision-making and highly coordinated actions to build the system, and *then* expect it to become decentralized.[54] Of course, transforming a centralized institution into a decentralized one will require those who wield power in a centralized organization to give it up, and a widely dispersed, divergent group to pick up pieces of that power—quite a significant ask.

If decentralization is aspirational for these systems, then they are currently similar to existing institutions with centralized power, but for some reason the builders of these systems claim they are different. Other than having a stated goal of becoming decentralized, there is no more reason to expect them to succeed in becoming decentralized than there is to expect existing institutions (e.g., banks) to transition from centralized to decentralized organizations.

G. Decentralization Can Be Used to Hide Power or Enable Rule-Breaking

Some commentators discussed how decentralization enables groups of people to obscure power and escape consequences for breaking rules.[55] Several discussed BitTorrent, which was able to continue operating despite threats to shut it down, and despite rampant copyright infringement through the use of the protocol.[56] As one former BitTorrent Inc. executive wrote recently, "if you're not Breaking Rules you're Doing it Wrong," in explaining the lessons BitTorrent holds for the crypto world.[57] Morris notes that "Decentralization in the sense it is applied to blockchain technologies . . . means creating an uncensorable system that enables the unfettered breaking of rules."[58]

As is well known, cryptocurrencies were initially associated with the criminal underworld of money laundering and the purchase of illicit goods and services on the Dark Web at sites such as Silk Road. Many still argue that these illegal activities represent the only real use cases for cryptocurrencies in the long term, as any lawful uses do not demand the ability to evade law enforcement, so can use more efficient centralized systems with known and accountable participants.

As I will discuss later on in the chapter, the term "decentralized" is being used to hide actions by participants in the system in a fog of supposedly "freely floating authority," and we must be vigilant not to overlook pockets of authority and power within these systems.

H. Calls to Action

The status quo usage of the terms "decentralized" and "decentralization" is deemed untenable by many commentators, and there are a variety of calls to action in the literature. Some simply call for deeper study of the term,[59] others propose frameworks for better understanding or measuring the decentralization of crypto systems,[60] while one proposes doing away with the terms altogether in discussing crypto systems.[61] The rationale behind these calls to action is that current usage of the term is creating misunderstandings about the capabilities of the technology. Further, it is clearly creating misunderstandings about how power works in these systems, with the potential for error in how law or regulation treats these systems and the people who act within them.

III. Examples of Concentrations of Power in Permissionless Blockchain Systems

Having demonstrated that "decentralization" is a problematic concept when applied to permissionless blockchains, in this Section III, I provide examples of actions within the Bitcoin and Ethereum blockchain systems that undermine claims that either system is particularly decentralized. A similar analysis could be done on every permissionless blockchain that exists (indeed, every single blockchain will be unique in this regard). In essence, I believe that many (including the SEC) are overlooking important sites of concentrated power within the Bitcoin and Ethereum systems (and potentially others), and instead are relying on simplistic views of decentralization to draw conclusions.[62]

These pockets of power include key developers and significant miners within the systems.[63] One could argue that every single line of code actually released to the network is an exercise of power by a particular software developer or small group of developers, as only a small number of developers (known as core developers) within a blockchain system have commit keys that enable them to make changes to the code repository. Every line of code reflects a policy choice about the blockchain system as a whole (e.g., how expensive should it be to participate in the system?) and technical choices about how to best reflect the policy mandate in code. (It is true that developers cannot compel anyone to run the software they release, but it is clear their influence is great.)

Run-of-the-mill software upgrades are not nearly as exciting as crisis software upgrades and clandestine meetings, however. The episodes I discuss later on in this section highlight moments where concentrations of power are vividly clear.[64] In Bitcoin, these moments include emergency rescues of the system by small groups of developers in the fall of 2018 (when a critical software bug was discovered) and in March 2013 (when the blockchain suffered an unintended hard fork). In Ethereum, these moments include the invite-only meetings held by key software developers in the fall of 2018 and the actions key developers took during the July 2016 hard fork in response to the DAO hack.[65] Power concentrations undermining claims of decentralization are also evident in the large portions of hashing power held by mining pools in each network. Finally, a series of 51% attacks on many permissionless blockchains, including the

January 2019 51% attack on Ethereum Classic, demonstrate the power dominant miners wield over these networks. In the following subsections, I discuss each of these issues in turn.

A. Critical Bug Discovery and Fix in Bitcoin Software in Fall 2018

On September 17, 2018, five developers of Bitcoin software were notified of a serious bug in several Bitcoin software clients, including Bitcoin Core, Bitcoin ABC, and Bitcoin Unlimited.[66] The bug could allow a denial of service (DoS) attack on Bitcoin, which could affect the security of the network. The five developers quickly shared the information with four other Bitcoin developers, one of whom realized that the bug actually had two potential implications, the second even more critical than the DoS vulnerability originally reported.[67] If exploited, the bug could enable someone to create Bitcoins out of thin air, in excess of the celebrated cap of 21 million. This "inflation bug" could devastate the cryptocurrency, undermining the public's faith in its credibility. The incident report from the software developers of Bitcoin Core, published several days later on September 20, 2018, makes for riveting reading, and includes this description of what happened after the discovery of the inflation bug (note the use of the passive voice):

> In order to encourage rapid upgrades, *the decision was made* to immediately patch and disclose the less serious Denial of Service vulnerability, concurrently with reaching out to miners, businesses, and other affected systems while delaying publication of the full issue to give times for systems to upgrade.[68]

The time log of events makes clear that at the time "the decision was made" to announce only the less severe bug implication and not the inflation implications, a maximum of 11 people knew about the inflation bug (it is unclear whether all the developers mentioned in the incident report knew of the inflation bug, or whether some were only informed of the DoS aspect of the bug).[69]

To be more explicit: fewer than a dozen people decided on September 17, 2018, to:

- withhold information about the critical implications of a bug from the public;
- prepare a patch that would fix both the DoS and inflation vulnerabilities;
- urge miners and nodes within the network to immediately install the patch on the basis that it fixed only a DoS bug; and

- disclose the critical inflation bug only after miners and others had upgraded with the ostensibly DoS-bug-only patch.

The developers only disclosed the critical inflation implications of the bug to the public on September 20, 2018—three days later.[70] As a quick reminder of the significance of their actions, on September 17, 2018, a Bitcoin traded for around $6,500 (U.S.), with a market cap of more than $108 billion.[71]

Further demonstrating the power of a select few within the Bitcoin system is the fact that the Bitcoin Core core developers initially contacted the "CEO of slushpool," one of the major Bitcoin mining pools, and within 20 minutes of the communication, the pool had upgraded to the recommended software.[72]

One could write many papers about the implications of this event,[73] but it is relevant to my argument in this chapter because it shows (in Hinman's words) "a . . . coordinated group . . . that is working actively to develop or guide the development of the infrastructure of the network."[74] Indeed, one could easily call the bug-fixing actions of this "coordinated group of [fewer than 12] actors . . . *essential efforts that affect[ed] the failure or success of the [Bitcoin] enterprise*."[75] If they hadn't fixed the bug immediately, the Bitcoin system faced potentially catastrophic failure. To be clear, I am not criticizing the people involved in the fix for the decisions they made to save the network, but it is evident that their actions are inconsistent with statements that the Bitcoin system is decentralized.

Perhaps one good rule of thumb for policymakers is that if some things have to be kept secret from others, the system is not decentralized. In Hinman's words, secrets held by a small number of developers indicate that "informational asymmetries exist between the promoters [defined broadly by Hinman to include developers] and potential purchasers/investors in the digital asset." Put simply, secrets reveal centralization.

As I have argued previously, moments of crisis uncover where actual power lies in a system.[76] In this case, the resolution of the Bitcoin inflation bug revealed the power concentrated in the hands of a few software developers, strongly undermining any claims that the system is decentralized. While Director Hinman could not have been aware of this particular action by Bitcoin developers when he delivered his June 2018 speech several months before the bug fix, this was not the first time a small group of Bitcoin developers acted to save the system.

B. Bitcoin's March 2013 Hard Fork

A similar rescue by a few Bitcoin developers occurred in March 2013, when Bitcoin experienced an unexpected fork of the network.[77] Nodes in the network were running different versions of software due to uneven upgrading to a new software release, and this caused the network to split in two. Upon discovering the fork, key developers determined which version of the forked ledger should be treated as the "real" Bitcoin and reached out to miners in the network to urge them to support the chosen ledger. To do so, some miners had to adopt the earlier software version, and lost earnings they had made on the rejected ledger. Once enough miners switched over, the network returned to a single ledger.

As with the 2018 inflation bug fix, the few software developers who acted to remedy the 2013 hard fork revealed their power within the Bitcoin system. These developers selected the authoritative ledger, creating winners and losers among the miners, depending on which version of the ledger they had been mining during the fork. Developers were able to communicate with particular miners and persuade them to run a particular version of software. These core developers, again, looked like a "coordinated group of actors . . . (whose) *essential efforts . . . affect[ed] the failure or success of the [Bitcoin] enterprise*."[78]

C. Secret Meetings of Ethereum Core Developers in Fall 2018

In the fall of 2018, during the DevCon conference in Prague, a group of key Ethereum software developers gathered to discuss potential upgrades to the system. The meeting was invitation-only, and, deviating from common practice for meetings or calls of the core developers, was not live-streamed. When news of the meeting broke to the rest of the Ethereum development community, there were immediate accusations of centralization and power grabs.[79]

In other multibillion dollar enterprises,[80] a strategy meeting of senior decision-makers would raise no eyebrows, but in a nominally decentralized, uncoordinated system that simply maintains open source software, holding analogous meetings is taboo. Amidst the uproar, different positions were aired, with some arguing that invite-only meetings were anathema to the ethos of open-source software development, and others arguing that leading developers needed the privacy to speak freely about possible risks and benefits of changes to the system, without the media immediately reporting and potentially twisting their words.[81] The issue remains unresolved, amidst efforts to better define how governance does and should operate within Ethereum. Notably, at least one Ethereum software developer meeting since the invite-only one was conducted under Chatham House Rules, enabling participants to speak freely without fear of attribution.[82]

Why would these invite-only meetings matter so much, and what do they have to do with the decentralization of the Ethereum system? In a word, everything. Permissionless blockchains like Ethereum run on open-source software and use common practices from grass-roots open-source software development to maintain, fix, and improve the software.[83] The claim made by open-source software developers is that no single person or group of persons are in charge of a given software client, but that changes to the code are made by achieving "rough consensus" about them. With open-source software, if one doesn't like the changes made in one version of the code, one can always copy the code and freely make whatever changes one likes. This process of copying the code and creating a new path for it is known as "forking" the code. In normal open-source software, forking may not have significant effect on others, but in permissionless blockchains, it has critically important effects, as the value of a token is tied to the strength of the network and community that runs its software. As we have learned over the last several years, forks of software in permissionless blockchains (and corresponding forks to networks) create new tokens, which are completely different beasts from the original token.[84] So, the way that software is developed matters hugely in permissionless blockchains, and the process is celebrated as not privileging some developers over others. As I've argued in the past, this is not a fair description of these systems, and disparate power inevitably resides in certain developers within them.[85]

Clearly, the discomfort and uncertainty about the governance process as well as what conversations should be open to the public stem from the importance that Ethereum (and Bitcoin, and really, any tokenized permissionless blockchain) has for those who use its tokens, build smart contracts on it, or otherwise rely on it as infrastructure. Core developers have the weight of the blockchain and its ecosystem on their shoulders, as their recommendations and the code they write can make or break the entire Ethereum system. Ironically, in systems that stemmed from a reaction against the power structures of the state and the financial system, concentrated power structures have re-emerged, forcing those with power to make similar decisions to those in traditional power structures (perhaps Ethereum core developers now have an inkling of why Federal Open Markets Committee Meetings are not held in public, and minutes are only released after a delay).

D. Ethereum's July 2016 Hard Fork

As has now entered crypto lore, the Ethereum blockchain hard forked in the summer of 2016 following the hack of the DAO, an application built atop it.[86] The hacker, exploiting a bug in the DAO's software code, was able to take the equivalent of around $50 million of Ether. The Ethereum developers decided to treat the hack as a theft, crafted a new version of Ethereum software to take the stolen Ether back from the hacker, and sold their solution to the miners and nodes of the Ethereum system. Though an advance poll of Ether holders or miners had sparse participation, the Ethereum developers decided to proceed with the hard fork.[87]

The results were mixed. A significant part of the network upgraded to the revised software and followed the new ledger (keeping the name Ethereum), and a smaller part Ethereum network rejected the upgrade and kept the old ledger (allowing the hacker to keep the stolen tokens) going under the name Ethereum Classic. The Ethereum Classic blockchain, with its token ETC, has since operated as an independent blockchain system.

How did the hard fork reveal concentrated power? The developers made numerous decisions that affected Ether holders and those with applications built on top of Ethereum (including, obviously, the DAO). These included whether to treat the hack as a theft justifying a remedy, how to get the funds back from the hacker, how to code the software to do it, and how to sell the solution to the Ethereum community.[88] Further, some members of the Ethereum community certainly perceived that the core developers had power, alleging that dominant developers had recommended the fork because they had personally lost money in the DAO hack.[89]

E. Hashing Power Concentration and 51% Attacks

The previous examples in this section dealt with concentrated power in small groups of software developers, but record producers (miners) within permissionless networks can also be sites of power. In blockchains such as Bitcoin and Ethereum, there are large mining pools that comprise significant portions of the hashing power of each network. A 2018 paper by Gencer et al. described the centralized nature of the Bitcoin and Ethereum networks, noting that more than 50% of the hashing power of each network was concentrated in just a handful of mining pools.[90] In proof-of-work systems such as Bitcoin and (currently) Ethereum, whoever controls more than 50% of the hashing power of the network effectively controls the validation process, and is able to block transactions from being entered onto the blockchain or even alter old entries on the blockchain (sometimes referred to as a block "reorg").

The power that miners and/or mining pools can wield through control of significant portions of hashing power has been on display over the past year, as a rash of 51% attacks has hit a number of cryptocurrencies (though not, as of this writing, Bitcoin or Ethereum). In January 2019, Ethereum Classic was the most prominent cryptocurrency yet to be hit by such an attack, resulting in a rewriting of its blockchain that enabled the attacker to steal over $1 million.[91] As with the software developers, miners and mining pools who control significant portions of hashing power sound a lot like "a . . . coordinated group . . . whose *essential efforts affect the failure or success of the enterprise*" they participate in.[92]

IV. Using "Decentralized" to Make Legal Decisions about Blockchains

In this section, I examine the implications for law of making decisions about permissionless blockchains based on their level of decentralization. They are significant, so regulators, courts, and lawmakers should tread carefully in using "decentralized" as a legal term. My analysis first draws from the foundations laid in Section II, focusing on the legal implications of (1) the uncertainty of the meaning of the term "decentralized"; (2) the fluid, dynamic nature of the "decentralization" level of a given blockchain; and (3) the aspirational nature of "decentralization" in today's permissionless blockchains. I then consider the implications of using the term "decentralized" to describe how power works in the system, given the many instances of the exercise of centralized power, a few of which are discussed in Section III. I argue that misconceptions about the decentralization of blockchain systems function as a veil over the critical actions of certain parties within the system, effectively shielding them from liability. Further, believing that power is diffuse when it is actually concentrated means that blockchain systems are more vulnerable to change than is commonly believed, which makes the tokens on them malleable rather than fixed. As we will see, this has potentially far-reaching implications.

A. Decentralization's Uncertain Meaning Makes It Ill-Suited for a Legal Standard

As I discussed in Section II, no one is sure what it means for a blockchain system to be decentralized, but they are sure the concept is complex, poorly understood, and difficult to quantify.[93] The system's decentralization is in part a description of its governance and part a description of the numerical, geographical, and ownership distribution of the computers within the network. (With the ownership of nodes relevant, governance seeps back into the node count aspect of decentralization, as well.)

We could certainly come up with complicated formulas to measure the "level of decentralization" of a permissionless blockchain system, as some commentators have suggested.[94] One could propose standards for determining a decentralization level in each of the relevant domains of a blockchain system (e.g., nodes, miners, developers, potentially exchanges), and then an aggregate measure of decentralization for the entire system that incorporates the measurements from all domains. One could propose that a node count over X (perhaps 100? 1,000? 10?) is considered decentralized within the node distribution domain. But, are those nodes controlled by a common party? Are they widely distributed geographically, such that they are less subject to common failure due to a natural disaster or a government action in a particular jurisdiction? For the node number to be meaningful, a lot of information about the nodes must also be collected and analyzed.

Further, how would we quantify the governance of software development? Count the number of developers? Look at how many people have commit access to the software repository? But, how meaningful would such a number be? It could be the case that doing this quantifies and purports to fix the meaning of something that is not measurable or necessarily meaningful.

I fear that making decisions, including legal decisions (as Hinman's speech suggests the SEC is doing), based on a simple assertion that a blockchain is decentralized is falling prey to the observational bias sometimes referred to as the "streetlight effect"—that is, paying attention only to matters that have been illuminated, and not ones remaining in the dark.[95] The name of the effect comes from the parable of the man who looked for his lost glasses only in places illuminated by a streetlight, not because he thought he had lost them there, but because that is where he could see. Here, the fact that the node networks of the Bitcoin and Ethereum systems are extensive and global is relatively well known and nodes are easily countable (in the gleam of the streetlight), while the roles of software developers, miners, and even nodes in governance are complex and poorly understood (in the shadows), so these actors who strongly influence the success or failure of a blockchain system remain unremarked.

Accounting scholars have recently termed this phenomenon "Gresham's Law of Measurement," stating it as: "Easy-to-calculate quantitative metrics tend to crowd out more relevant but difficult-to measure assessments."[96] Ramamoorti et al. note that "succumbing to the Gresham's Law of Measurement means allowing measurability to trump meaningfulness. In other words, easily calculated quantitative metrics may provide the illusion of measurability while in actuality not being meaningful."[97] Here, it is relatively easy to count nodes in a network, but much harder to identify and understand how miners, nodes, and software developers interact in governing a blockchain.[98] As Sarah Jamie Lewis, a privacy advocate and crypto systems expert, has explained, "We need to move beyond naïve conceptions of decentralization (like the % of nodes owned by an entity), and instead, holistically, understand how trust and power are given, distributed and interact . . . Hidden centralization is the curse of protocol design of our age. Many people have become very good at obfuscating and rationalizing away power concentration."[99]

The lesson for the SEC and all others making legal or regulatory decisions about crypto systems is that we should not "regulate by streetlight," but should actively work to discover the facts before making legal or regulatory decisions, even if the facts are hidden and ambiguous.[100] The decentralization of a given blockchain system is such a complex, undefined concept that it is a bad idea to use it to make legal decisions at this point in time. Legal decisions based on the concept will sit on faulty foundations, making them difficult to defend and potentially opening them up to accusations of bias.

B. Decentralization's Dynamic Nature Complicates Its Use as a Legal Standard

The always-changing nature of a blockchain system's level of decentralization also makes it problematic to use "decentralized" as a basis for legal decisions. As I described in Section II, the "decentralization" level of a blockchain system (whatever one determines "decentralized" to mean) is a fluid characteristic.[101] This is because the domains within blockchain systems that are relevant to the concept of decentralization are constantly changing. The number of nodes in a blockchain system fluctuates, as people enter and exit the system at will with their computers (in a "permissionless" system, no permission is needed to participate in or leave the network). The hashing power and its distribution change frequently as miners go on and offline with their hashing power based on whether the price of the cryptocurrency makes it financially attractive to continue to provide transaction processing. The people serving as core developers of crypto systems are also in flux, as people gain or lose the trust of their peer developers or resign due to overwork, low (or no) compensation, or perceived risk of liability. Each of these domains is fluid, and helps to constitute the power distribution of the network. This means that if a system's level of decentralization is used to make legal decisions, each category would arguably need to be measured or evaluated periodically to see if that particular domain remains "decentralized."

Of course, the mere fact that a quantity or characteristic changes over time does not mean that law cannot address it. In a world characterized by constant change, humans have constructed ways for law to address change. For instance, as people age, certain of their legal rights and responsibilities also change. People become able to make binding contracts once they turn 17, for instance (depending on the state), or are able to vote once they turn 18, or are able to qualify for certain retirement benefits once they turn 65. As people's health, employment, income, or marital statuses change, for example, they may qualify for certain government benefits or tax consequences. Certain of these statuses are easily measurable (e.g., there is a magic moment when one turns 18 or becomes married), while others are not (e.g., disability is notoriously hard to measure, and requires input from doctors, the person claiming disability, and others). The question is whether "decentralization" is an easy-to-measure characteristic or a fuzzier, hard-to-measure one. I'd lean toward fuzziness, at least if we incorporate the governance that occurs through the software development process.

If a system's level of decentralization were relevant to a legal status, there would have to be periodic evaluations of the decentralization level of the relevant blockchain system to measure it. This raises questions about what happens if the decentralization level of a system decreases (i.e., the system centralizes) *after* the system has previously been deemed sufficiently decentralized to achieve a particular legal status. Using Hinman's statement that Ether is not a security because Ethereum is "sufficiently decentralized" as just one example of the complications that arise, we wonder, could Ether become a security in the future if it stops being "sufficiently decentralized?" Can something cease to be a security that has already been one?[102] How? What are the rules for trading it? How is secondary market trading of the token managed when the token can fluctuate between security and non-security? And if the measurement and determination of a decentralization level is done periodically to mark the moment when a particular legal status is achieved, then participants in blockchain systems (nodes, miners, developers) may game the standard by taking actions to move along the decentralization spectrum. If the prize is large (as non-security status would be), then anything gameable (including a level of decentralization) will be gamed.

C. If Actual Decentralization Is Now Just a Dream, Wait Till It Comes True

In Section III, I provided examples of events in Bitcoin and Ethereum that belie claims that they are decentralized, while in Section II, I noted the largely aspirational nature of "decentralization" in permissionless blockchains. If this is the case, it is premature to use "decentralization" as a way to make legal decisions. However noble the goals are for a given blockchain system to reach decentralization nirvana, the law must deal with present-day realities rather than hopes or dreams.

D. Decentralization Veils and Malleable Tokens

In this section, I discuss how using the "decentralization" of a blockchain system to make legal and other decisions about its token can result in flawed choices from both a legal and a risk perspective. This is because, when "decentralized" is used in its mainstream sense of inevitably indicating diffused power, it may mischaracterize or overstate how free of concentrated power the system is. Misunderstandings about how power works in the system, masked by simply describing the system as "decentralized," can then infect any decisions based on the decentralization of the blockchain.

Over the course of this chapter, I have sought to convey that despite the common use of "decentralized" to indicate that power is diffuse rather than concentrated in a blockchain system, existing blockchains such as Bitcoin and Ethereum have small coordinated groups who shape how the systems operate. To be explicit, though they are called "decentralized," there are many parts of blockchain systems that are exceedingly centralized. Thus, the meaning commonly conveyed by the word "decentralized" does not match the reality of these systems, with the consequence that misleading, inaccurate information about how power works in a given blockchain system is being conveyed every time someone describes the system as decentralized. This includes regulators, policymakers, and anyone else making decisions about these systems.

In the subsections that follow I argue that misuse of the term "decentralized" can lead to (1) flawed judgments about how accountability or liability of people within a blockchain system should work, effectively providing a liability shield similar to that of limited liability entities; and (2) perceptions that the tokens of a given system are more fixed and less subject to change than they are, potentially impacting any financial product tied to that token as well as other infrastructure built on or related to the blockchain system.

1. Who Needs an Entity When You've Got a Veil of Decentralization?

My argument here is simple: the common meaning of "decentralized" as applied to blockchain systems functions as a veil that *covers over and prevents many from seeing* the actions of key actors within the system. Hence, Hinman's (and others') inability to see the small groups of people who wield concentrated power in operating the blockchain protocol. In essence, if it's decentralized, well, no particular people are doing things of consequence.

Going further, if one believes that no particular people are doing things of consequence, and power is diffuse, then there is effectively no human agency within the system to hold accountable for anything. If you *can't see* people doing things that are "a key determining factor in the enterprise," then how could you hold anyone accountable for illegal actions taken or facilitated by the system, or for failures of the system?[103] There simply are no people to be found to punish or to task with responsibilities, such as, in the context of the securities laws, making disclosures to investors. Law has no reason to reach into such a system, as there is no relevant human behavior to direct. The consequence of casting a veil over the people's actions is that they may not be held accountable for those actions—in effect, that a *Veil of Decentralization* functions as a liability shield akin to the famed corporate veil.[104]

Moreover, being protected by a Veil of Decentralization may even be better than what blockchain participants could get if they actually formed a limited liability entity together. In entities, people making significant decisions that affect others (such as directors, officers, or managers) generally owe fiduciary duties, but, despite my urging, no one has yet decided to treat the core developers or significant miners of blockchain protocols as fiduciaries.[105] What's more, the Veil of Decentralization is helpful to participants in the blockchain because it provides a liability shield without making the blockchain system a legal person that could be sued.[106] With a limited liability entity, the corporation or LLC provides the site of legal personhood, but with a decentralized blockchain system, there is no such site.[107] Thus, if we misapply the term "decentralized," people within "decentralized" blockchain systems get the benefit of limited liability without the cost of certain duties and responsibilities.

Note that I am not arguing that Hinman or other regulators are intentionally creating a variation on the corporate form for decentralized blockchain systems, but that this backdoor entity creation is a byproduct of misunderstandings of how power works in the systems, hidden by the use of the term "decentralized."

Clearly, it is problematic to inadvertently give a group of people acting together what is arguably the core benefit of organizational law[108] without demanding any of the obligations organizational law generally requires in return. As Usha Rodrigues reminds us, "only organizational law can create impermeable barriers to protect the firm's participants from claims outside the firm."[109] Similarly, Dirk A. Zetzsche et al. note,

> First, in general, law covers all relations among people and items owned and controlled by them. There is no carve-out for cooperation in a distributed ledger. Second, no legislature is likely to enact an exception to this catch-all characteristic of law as it would promote irresponsible behavior by those controlling the distributed ledger. No legal system could afford a carve-out for DLT interactions given the loopholes it would create.[110]

Yet, a backdoor "carve-out for cooperation in a distributed ledger" is arguably what blockchain protocol actors receive if they are protected from accountability by the Veil of Decentralization.

This is all occurring as scholars grapple with the appropriate legal treatment for the group of people acting together in a blockchain system.[111] Karen Yeung points out that "[t]he decentralized, distributed nature of public blockchains means that there is no single, centrally controlled and integrated entity which conventional legal systems can readily identify as potential bearers of legal rights and/or duties. This may generate difficulties for conventional law-makers . . . "[112] Yeung explains how a corporate entity gives law an access point to address rights and duties, "[y]et, unlike stakeholders in a corporation, participants in blockchain networks are not recognized by law as bound together in a single, centralized organizational form."[113] Philipp Hacker similarly wrestles with legal accountability within blockchain systems, arguing that permissionless blockchains should adopt a tailored corporate governance framework that specifies the duties of software developers and miners or face legal consequences (in what he terms a "comply or explain" approach).[114]

Solutions to the blockchain entity dilemma have been proposed. Carla Reyes rejects the default partnership as an appropriate legal entity for a blockchain protocol such as Bitcoin or Ethereum because of concerns that holders of the tokens of the blockchain could be treated as partners of the miners, exposing them to unexpected joint and several liabilities.[115] She also worries that the creators of blockchain protocols (i.e., software developers) would similarly be viewed as partners (with accompanying liability), which she believes would stifle innovation.[116] Reyes asserts that the common law business trust would be a better legal form for "certain decentralized or distributed business entities" (which she terms "DBEs"), arguing that the miners act as trustees of the blockchain record through their validation efforts and holders of tokens (such as Ether or Bitcoin) function as beneficiaries.[117] In this way, she envisions the DBE (i.e., the blockchain system) obtaining legal personhood, limited liability, and other benefits equivalent to the corporate form. Another reason Reyes views the business trust as appropriate for blockchain protocols is that some states do not require filings to establish the business trust, which is important because affirmatively availing a "decentralized" blockchain system of state legal structures may be taboo to many participants in the protocol.[118] In this case, the default business trust could come to the rescue of the blockchain participants, unlike the much less protective default partnership.

The State of Vermont has similarly considered the issue and in 2018, enacted legislation that creates a new business entity called the Blockchain-Based Limited Liability Company—the BBLLC.[119] Like the common law business trust Reyes proposes, the BBLLC would provide a blockchain protocol with limited liability. It also would impose concomitant duties on participants in the system.

I do not take a position on which is the best legal form for a permissionless blockchain system, as that is outside the scope of this chapter. What is important to recognize is that policymakers should be doling out entity-type benefits only *after* carefully deliberating and determining an appropriate balance of rights and liabilities. It is critically important to get this designation right, as it will affect the behavior of participants both inside and outside these systems, and may very well determine whether blockchains are a success or a failure. Notably, treating blockchains as de facto limited liability entities for some purposes and not others means that rights and liabilities are not aligned. In all solutions proposed by Reyes, Hacker, and the Vermont BBLLC, there is an effort to balance the benefits of limited liability with certain obligations of those within the system. This will almost certainly not happen if we inadvertently treat the system as providing limited liability due to the Veil of Decentralization.

As we've seen in numerous domains, permissionless blockchains make us rethink our existing structures from the ground up. Here, the core question is how a group of people running a common system should be treated from a legal perspective. Should they all be individually responsible for the actions of the system? Should none of them be individually responsible for the actions of the systems, if there is not a single party with absolute control? The most difficult and interesting question raised by Hinman's suggestion that the decentralization level of a blockchain system should drive legal decisions is how we should treat group activities that do not fit into one of our existing legal categories.

Law generally uses legal fictions such as corporations, limited liability companies, or partnerships to structure how we treat groups of people. This is useful because the legal entities enable the parties operating through them to define precisely their potential liabilities, rights, and responsibilities. We know how to treat the group of people because they have put themselves into a particular box, and we have specified how that box works. Permissionless blockchain systems do not fit obviously into those boxes, or at least the people operating within them have sought to exist outside of them. In deciding which "box" to put these systems in (or whether they need an altogether new box), we must engage intentionally with the question and avoid acting based on misunderstandings. We must peel away the Veil of Decentralization and dig in.

2. If People Wield Unnoticed Power, Tokens Are Unexpectedly Malleable

The final significant consequence of misusing "decentralized" that I will discuss is the risk it creates due to misunderstandings about how tokens on these blockchain systems behave. Again, my argument here is straightforward. Misunderstandings about how power works in a blockchain system, conveyed through uncritical use of the term "decentralized," can mean the systems (and the tokens on them) may behave differently than we expect them to. If we believe that power is diffuse within the system, then it should be difficult to make changes to the system, and therefore to the token that rides on the system. But, if power is concentrated, then changes to the system are easier to make, and the corresponding tokens may be more fluid than we think.

This is significant, as legal and risk determinations about tokens such as Bitcoin and Ether have generally been based on the view that, while the trading in the token may be subject to manipulation in immature, semi-regulated markets, the tokens themselves have fixed characteristics. For instance, Bitcoin is valued by some because of its famed cap of 21 million tokens, which is treated as a fixed characteristic. The Commodity Futures Trading Commission has deemed Bitcoins to be commodities,[120] implying that the Bitcoin token is a thing with a stable set of characteristics, rather than one whose most basic characteristics could shift based on the whims of a few. This view of tokens as having fixed characteristics undergirds decisions to offer futures contracts based on tokens, and to otherwise integrate tokens such as Bitcoin and Ether into the mainstream financial system, whether as collateral for loans or investments by retail and institutional investors.

Yet, as this chapter has sought to show, power is not necessarily diffuse in a permissionless blockchain just because it is labeled "decentralized." And the consequence of power concentrations may be sudden changes to the system and its tokens. Hacker puts it well:

> [T]he decentralized structure [of a blockchain system] is vulnerable to coalitions of the willing, which combine enough technological prowess, computing power, or force of persuasion to implement their proposals on the development of the blockchain. This leads to erratic, unforeseen and potentially radical changes of the system status as a reaction to external shocks or internal developments.[121]

In his analysis of cryptocurrency systems through the lens of complexity theory, Hacker describes how immature governance within blockchains "leads to an inherent unpredictability of the future development of the protocols when coalitions of major players (core developers, operators of mining pools) can exert disproportionate power to unilaterally push updates they view as personally favorable or generally reasonable."[122] Further, he asserts that "we should expect to see more unpredictable behavior over time; this implies radical uncertainty for cryptocurrencies and token-based ventures built on top of them."[123]

"Radical uncertainty" around systems that serve as infrastructure is a troubling prospect. When blockchain systems such as Bitcoin or Ethereum serve as infrastructure to applications built atop them, and their tokens are integrated into the financial operations of our societies, sudden changes to the infrastructure (tied to the exercise of centralized, unaccountable power) can be destabilizing to everything that rests on the infrastructure.[124] As Vidan and Lehdonvirta note, "one of the key characteristics of infrastructure is its invisibility up to the point of breakdown, when its otherwise taken-for-granted components come under scrutiny. In Bitcoin, these breakdowns reveal centers of power in the ostensibly decentralized machinery of the cryptocurrency."[125]

If the systems and their protocols are highly unpredictable due to unpredictable exercises of centralized power by people within the system, then the characteristics of their tokens are much more fluid than is commonly understood.

A token looks less like a rigid steel box with defined characteristics (analogous to the legal entity structures I discussed earlier), and more like a lump of clay that can be reshaped at any moment. This means that any risk analysis and decision made based on the idea that a token is like a steel box is flawed. If a token is a shapeshifter rather than a "thing" (i.e., it remains constantly subject to alteration by unexpected changes to the underlying protocol), then legal or regulatory judgments that are based on it looking like a steel box (i.e., that it is stable and impervious to human manipulation) are very likely wrong. This misunderstanding could potentially impact the token's status as a commodity, a security, or as money itself. Further, as tokens become integrated into the mainstream financial system through their integration into financial products such as futures or exchange traded funds, or as collateral for loans, or as investments by hedge funds, pension funds, or endowments, the implications become greater.

To be clear, it is the *flawed perception* of the power dynamics of permissionless blockchain systems that is the source of errant risk assessments. If our understandings of the power dynamics within a system were accurate, we would expect fluidity in the characteristics of a token, and therefore factor that fluidity into our risk assessments, our views of the value and potential use cases of the technology, and critically, our legal and regulatory decisions. My argument is that unquestioning use of the term "decentralized" and the romanticization of "decentralization" helps to create, sustain, and spread false beliefs about blockchain power structures. In other words, the Veil of Decentralization strikes again.

V. Closing Reflections

Spurred by Director Hinman's statement that Ether is not a security because Ethereum is "sufficiently decentralized," in this chapter I have argued that the terms "decentralized" and "decentralization" are misleading in suggesting that that permissionless blockchains lack sites of concentrated power and human agency. To the contrary, there have been many actions taken by small, coordinated groups of people that have made pivotal changes to the Bitcoin and Ethereum systems. The bug fixes, secret developer meetings, and mining pool concentration discussed in Section III all reveal sites of concentrated—rather than diffuse—power. Yet in uncritically describing blockchain systems as decentralized, we skip over all of that.

This is no mere pedant's lament. In Section IV, I argued that it is highly problematic to use "decentralized" as a legal standard for a variety of reasons from our poor understanding of the concept, to its inevitably shifting nature. Most critical, however, is the fact that the Veil of Decentralization, as I call it, may lead us to inadvertently provide the benefits of organizational law (limited liability) to a blockchain structure or to make decisions about tokens based on misconceptions of how power operates within a blockchain system. Both of these could potentially cause serious harm, as a lack of accountability without corresponding duties is a recipe for high-risk behavior, and "radical uncertainty" in a token's characteristics could impact every matter tied to that token.

In the end, it is all about obtaining a clear-eyed understanding about how power actually operates within the systems, and making decisions based on that enlightened understanding. As we should know by now, failure to appreciate how power works in a given system can have serious consequences. We are dissatisfied now with how power works on the internet—with the long-unappreciated concentrations of power that have grown up in platforms such as Google and Facebook. This is in large part because we believed that the characteristics of these systems were as they were represented to the public. They were free, about connecting the world, and serving their users. Finding out now that (as long-ignored critics perceived) users of these systems are exploited, manipulated, and surveilled through the platforms is extremely upsetting, and is leading to calls to regulate or break up these platforms. If we had demanded that the data mining and tracking that digital platforms do be openly described and publicly debated, we might have ended up in a different place. (Of course, maybe not, as maybe we as busy humans are too distracted or apathetic to resist the siren song of the free "services" of Facebook or Google.)

We need to be cautious about embracing the new utopianism of "decentralization"—this time through a blockchain world. As others have noted, this feels like a second chance to get the power dynamics of our digital activities *right*. This can only happen, though, through active interrogation of how power operates in *each* blockchain system. We must push back when presented with think pieces and thought leaders that fantasize about the better world we'll have if it is "decentralized." These utopian visions generally gloss over what "decentralization" would really mean in a particular, specific blockchain system, and simply jump to the amazingness of a world based on "decentralization." (So, jumping ahead to the "what if we had it" before figuring out what the "it" is.)

Finally, this chapter does not attempt to define "decentralized" or "decentralization" for blockchain systems. We're just not there yet. It seeks, alternatively, to illuminate how tenuous a grasp we have on the concept, that the reality of existing systems may not match the rhetoric about their decentralization, and the significant consequences of using this concept to make legal and other decisions based on our existing limited understanding. It's possible that I will attempt to define decentralization in permissionless blockchains in future work, but at the moment, I feel too much technology development and research is needed before that would be useful. For now, I'm in full support of Tony Sheng's recommendation that we "ditch [the term] "decentralization."[126] Maybe, in the end, that would help us lift the veil.