Ketsal

Ketsal Open Standards

Data Points to Measure Blockchain Network Centralization

October 21, 2020

Josh Garcia[1] Jenny Leung[2]

Abstract: Developers of blockchain networks often seek "decentralization" as an end goal. Put another way, they tend to eschew centralized solutions when building platforms meant to avoid intermediation. Similarly, outside observers place value – philosophical, economic, or otherwise – in whether a network is "decentralized." Yet no definition exists for "decentralization." Where the term means "not centralized," "centralized" itself similarly lacks definition. To have decentralization as an end goal often means aiming for a vague, and possibly moving, target. In the spirit of clarifying what, exactly, developers might want to achieve as their network matures, we propose standard, objective measures for three forms of "centralization." Once "centralization" has data points acting as its guard rails, it makes more sense to say a network is "not centralized." Further, concrete data points can form the basis of a standard dataset one can use to compare "centralization" across blockchain networks. The discreteness of the data points may also allow developers of new networks to set tangible goals.

We parse blockchain networks into three layers: computational (focusing on nodes trading data), economic (focusing on network addresses trading value), and political (focusing on persons trading communications regarding network governance or control). We then list data points that may provide valuable information regarding one or more of these three layers and those less likely to yield useful or unique information regarding these layers. We provide detailed rationales for measuring the former and for not measuring the latter. In the appendix, we provide values for data points (where available) regarding the Bitcoin network.

The authors are grateful to Zachary Fallon (Ketsal), Zach Finzi (Inca Digital), Nicholas Gans (Inca Digital), Lane Rettig (Independent Researcher), and Diana J. Stern for providing critical feedback on this document. Nothing in this document should be construed as legal advice.

[1] Principal and Co-Founder, Ketsal PLLC. Adjunct Professor, University of Michigan Law School.

[2] Attorney, Ketsal PLLC. Former Regulatory Attorney, Australian Securities and Investments Commission.

Introduction

Many blockchain developers aim to build a "decentralized" network but cannot point to any clear definition of "decentralization." We propose below a set of open standards that interested parties can use to determine "centralization," with the goal of bringing more meaning to the phrase, "my blockchain network, DeFi project, or other application is not centralized." These standards take the form of objective, data-driven metrics that measure an aspect of centralization along three different layers of a blockchain network.

We foresee a range of use cases for these metrics. Developers – whether they build new protocols or decentralized applications on top of existing ones – may seek to use this framework to set goals towards "decentralization" or "network maturity" on their roadmaps or to identify hard milestones for investors. State and national banks that wish to custody cryptocurrencies may seek to use certain metrics in determining whether the bank custodies a security or a commodity for a client (and what risk management processes should apply to the asset as a result).[3] Cryptocurrency exchanges may seek to automate review of these metrics to monitor whether economic control over a blockchain network's assets is at imminent risk of becoming centralized – and may want to warn users of that risk or halt trading temporarily until the risk subsides. Code auditors and security specialists may wish to focus review on computational metrics to ensure no centralized control exists over the majority of a blockchain network's nodes.

Our approach acknowledges that any network is a system of vertices and edges, whether biological, mathematical, social, or computational. We view blockchain networks as possessing three associated layers:

1. **Computational** – A network of computational units which process and transfer data via protocols. Their interaction is constrained by both code and technological requirements.
2. **Economic** – A network of blockchain network addresses which actually passes value between each other with defined financial constraints. This layer contains the monetary policy and transaction validation rules allowed by a network's consensus protocols.
3. **Political** – A network of persons[4] communicating with each other regarding network governance and control. This layer contains the networks' governance protocols, as well as the essential managerial control that persons have over, or the essential managerial contributions that persons make to, the underlying digital asset network.[5]

---

[3] Office of the Comptroller of Currency, *National Bank and Federal Savings Association Digital Activities*, 85 Fed. Reg. 40827 (proposed June 4, 2020) ("Banks should also be aware that different cryptocurrencies may have different technical characteristics and may therefore require risk management procedures specific to that particular currency.").

[4] All references to "person" or "persons" for the purposes of this document, includes natural persons, corporations, and other organizations.

[5] *See generally,* Token Engineering, *Token Engineering Fundamentals | Michael Zargham & Matt Barlin, BlockScience,* Youtube (Jun. 5, 2018), https://youtu.be/DsRG9uZmME8; Shumo Cho and Sophia Wang, *The Curses of Blockchain Decentralization* (Oct. 6, 2018), https://arxiv.org/pdf/1810.02937.pdf; Adam Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks* (Mar. 29, 2018), https://arxiv.org/pdf/1801.03998.pdf; Sneha Goswami, *Scalability Analysis of Blockchains Through Blockchain Simulation* (May 2017), https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3979&context=thesesdissertations; and Paul Sztorc, *Measuring Decentralization* (Sep. 9, 2015), http://www.truthcoin.info/blog/measuring-decentralization/.

The computational layer enforces the rules established within the economic layer, which in turn facilitates the activities of the political layer. We conceptualize these network layers as being made of a different substrate, each with discernible vertices and edges.

Layer	Vertices	Edges
Computational	Physical computers ("**nodes**").	Packets of information sent between nodes.
Economic	Blockchain network addresses with value.	Value transfer between addresses and the value of the asset transferred.
Political	Persons.	Communications between persons regarding network governance or control.

Each of these network layers can have varying degrees of centralization.[6] For instance, a network's political layer can be centralized if most political activity (communications regarding network governance or control) occurs among a small number of political vertices (natural persons, corporations or other organizations). The economic layer can be said to be centralized if most economic activity (value transfer) occurs among a small number of economic vertices (network addresses). And the computational layer may be centralized where most computational activity (data transfer) occurs among a small number of computational vertices (nodes).

Use of a Standard Dataset

The dataset for each layer will only be useful to the extent a specialist seeks to better understand the level of computational, economic, or political centralization of a network. For example, information security auditors or researchers may wish to review the computational centralization of a network operational for two years and, using a standard dataset, compare the results to a network operational for five years. Market makers, cryptocurrency exchanges, and other liquidity providers may wish to review the economic centralization of a network to determine financial risks in trading in or listing a token. Regulators and compliance specialists may wish to review political centralization as part of a standardized *Howey*[7] analysis, or, in the future, to determine whether a network is "sufficiently decentralized"[8] or has obtained "network maturity."[9]

The list of data points below implies the availability of data for each item on the list. The platform Nakamoto Terminal ("**NTerminal**"), created and operated by Inca Digital, is a data aggregation

---

[6] *See* Martin Walker, Distributed Ledger Technology: Hybrid Approach, Front-to-Back Designing and Changing Trade Processing Infrastructure (2018).

[7] *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

[8] *See* William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic)* (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418 ("**Hinman Speech**").

[9] *See* Hester Peirce, *Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization* (Feb. 6, 2020), https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06 ("**Peirce Proposal**").

and analytics platform that we used to develop the list of proposed data points. We have included a report for the Bitcoin network in the Appendix, some of which makes use of NTerminal data.

Benchmarks

Any objective measure of a dataset benefits from useful benchmarks. We reference the Bitcoin network and the Ethereum network as such benchmarks ("**Benchmark Networks**") in this document. These two networks are widely considered "decentralized."[10] In addition, they are also considered relatively safe and secure,[11] an important consideration for an analyst seeking to interpret a computational centralization dataset. Benchmark Networks have relatively liquid markets,[12] an important consideration for a market maker or exchange interpreting the economic centralization dataset. Also, the Benchmark Networks have been deemed by U.S. regulators to host native assets that are not securities,[13] one of the few official tentpoles available for someone reviewing the political centralization dataset as part of a *Howey* analysis.

Key Source Materials

We used Vitalik Buterin's 2017 Medium article.[14] espousing three types of decentralization as a starting point. Multiple conversations with NTerminal between April 2019 and June 2020 proved crucial to refining our understanding of the substrates in a blockchain network and developing a working list of data points. The plain language of *Howey* and its eponymous test, along with guidance issued by the Securities and Exchange Commission ("**SEC**") regarding blockchain networks,[15] also proved helpful in in narrowing data points relevant to the political layer.

---

[10] *See, e.g.*, Adam Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks* (Mar. 29, 2018), https://arxiv.org/pdf/1801.03998.pdf (noting that "Ethereum nodes are not accumulated in a single geographical region, but are more evenly distributed around the world" and that "the Bitcoin network is geographically more clustered than Ethereum, with many nodes likely residing in datacenters.").

[11] *See, e.g.,* Joseph Regan, *3 Reasons Bitcoin is (mostly) Safe* (Feb. 22, 2019), https://www.avg.com/en/signal/is-bitcoin-safe; Gavin Wood, Ethereum: *A Secure Decentralised Generalised Transaction Ledger* (last accessed Mar. 21, 2020), https://gavwood.com/paper.pdf.

[12] *See* Samuel Haig, *Top Cryptocurrencies Are Exponentially More Liquid Than Ever Before* (Feb. 20, 2020), https://cointelegraph.com/news/liquidity-of-top-cryptocurrencies-is-stronger-than-during-2017-bull-market.

[13] *See, e.g.* Hinman Speech ("... current offers and sales of Ether are not securities transactions."); Press Release, NYDFS, *DFS Advances New York's Thriving Virtual Currency and Money Transmitter Licenses to Tagomi Trading, LLC* (Mar. 27, 2019), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1903271 ("DFS has authorized Tagomi to engage in money transmission and to offer trade routing and order execution services for non-securities virtual currencies, including Bitcoin, Ether, Bitcoin Cash and LiteCoin."); and Letter from Brent J. Fields, Disclosure Review and Accounting Office, SEC, to Jacob E. Comer, Cipher Technologies Management LP (Oct. 1, 2019), https://www.sec.gov/Archives/edgar/data/1776589/999999999719007180/filename1.pdf (" . . . and we disagree with your conclusion that bitcoin is a security.").

[14] Vitalik Buterin, *The Meaning of Decentralization*, Medium (Feb. 6, 2017) https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274. Note we diverge in material respects from Buterin's original formulation.

[15] Framework for "Investment Contract" Analysis of Digital Assets, SEC Staff Guidance at 4 (Apr. 3, 2019), https://www.sec.gov/files/dlt-framework.pdf (the "**SEC Framework**").

Computational Centralization – Measuring Computers

Security concerns predominate when designing any blockchain network – the primary goal of which is to have no central point of failure.[16] In the early days of network design and testing, some developers may wish to have fewer physical computers (nodes) form the basis of an underlying blockchain network. In such cases, computational centralization would present itself early in the blockchain network's lifecycle. As the network adds more nodes, computational centralization would diminish.

The computational layer identifies nodes as the relevant vertices, yet nodes are often controlled by natural persons. Thus, data points primarily relevant to computational centralization may also be secondarily relevant to the other two layers. Further, while not traditionally useful to a *Howey* analysis, computational data points may be useful for determining when a network is "sufficiently decentralized" or has reached "network maturity" from a securities laws standpoint,[17] understanding those terms have yet to be formally defined by securities regulators.[18]

When we state a blockchain network is "centralized" with respect to its computational layer, we mean to say, as compared to a Benchmark Network, a relatively small number of nodes sends packets of information to each other.

Economic Centralization – Measuring Market Power

The economic layer focuses on network addresses. Yet as above, network addresses are ultimately controlled by persons, and thus some economic data points may be relevant to political centralization. For instance, a regulator looking to economic data points might ask whether participants on a network may be led to rely[19] on the managerial efforts of others to see either (i) value of the native asset increase, or (ii) profits flowing back to holders of the native asset.[20] Where fewer persons control an asset's economics, a regulator may more likely view purchasers of a network's native asset as "relying on the managerial efforts of" those economic powers for

---

[16] *See, e.g.,* Vitalik Buterin, *The Meaning of Decentralization*, Medium (Feb. 6, 2017) https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 ("Attack resistance - decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system"). *See also* Lamport et al, *The Byzantine Generals Problem* (July 3, 1982), https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf.

[17] *See* supra note 13.

[18] *See* Peirce Proposal (defining "network maturity" as the status of a decentralized or functional network that is achieved when the network is either (i) Not controlled and is not reasonably likely to be controlled or unilaterally changed by any single person, entity, or group of persons or entities under common control; or (ii) Functional, as demonstrated by the ability of holders to use tokens for the transmission and storage of value, to prove control over the tokens, to participate in an application running on the network, or in a manner consistent with the utility of the network.); and Hester Peirce, *Hester Peirce: Tell Me How to Improve My Safe Harbor Proposal,* (Feb. 18, 2020), https://www.coindesk.com/hester-peirce-tell-me-how-to-improve-my-safe-harbor-proposal (recognizing the lack of a bright-line test for whether a token is a security at the end of three years.).

[19] *See, e.g., SEC v. C. M. Joiner Leasing Corp.*, 320 U.S. 344, 353 (1943) and *In re Munchee, Inc.*, Securities Act Rel. No. 10445 (Dec. 11, 2017) ("**Munchee**") ("Because of the conduct and marketing materials of Munchee and its agents, investors would have had a reasonable belief that Munchee and its agents could be relied upon").

[20] *See, e.g.,* Forman ("By profits the Court has meant either capital appreciation resulting from the development of the initial investment [or] a participation in earnings resulting from the use of investors' funds.").

an expected value increase.[21] In the future, data related to economic centralization may be more directly useful for determining if a network is "sufficiently decentralized" or has achieved "network maturity" from a securities laws standpoint,[22] understanding, again, those terms lack a formal definition.

When we state a blockchain network is "centralized" with respect to its economic layer, we mean to say, as compared to a Benchmark Network, a relatively small number of network addresses containing a significant portion of the circulating value actually stores that value, or sends that value to each other.

Political Centralization – Measuring Influence

The political layer focuses on persons. Political centralization in a blockchain network can be measured by reference to its governance design, the distribution of control across its mining or voting community ("**Voting Control**"), or the distribution of control over protocol-level changes ("**Change Control**"). Governance design is less easy to reduce to data points; Voting Control and Change Control lend themselves better to such reduction.

The authors of this report are lawyers who recognize that, where fewer persons control the most critical features of a blockchain network, it is more likely purchasers of that network's native asset can be said to rely on the essential, managerial efforts of others in some manner. The concept of "reliance on the managerial efforts of others" reigns as a longstanding and crucial component to the investment contract analysis under U.S. federal securities laws,[23] and continues to be relevant to any *Howey* inquiry for digital assets.[24] For instance, developers have sold rights to a native asset prior to its existence and have complete control over the development of the as yet incomplete network. Regulators often view such sales as consisting of the sale of investment contracts because purchasers are arguably relying on the developers' efforts to derive a profit from owning rights to the asset or the asset itself.[25]

---

[21] *See, e.g.,* Jay Clayton, Chairman, Securities Exchange Commission, *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC* (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission ("Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law."). *See also* Munchee and *In re CarrierEQ, Inc. d/b/a Airfox*, Securities Act Rel. No. 10575 (Nov. 16, 2018) (**"Airfox**") (finding a reasonable expectation of profits in part because "AirFox highlighted to investors that it would ensure secondary trading market for AirTokens shortly after the completion of the offering and prior to the creation of the ecosystem, including taking steps to list AirTokens on multiple digital token trading platforms.").

[22] *See supra* note 13.

[23] *See*, e.g., *SEC v. C. M. Joiner Leasing Corp.*, 320 U.S. 344 (1943); *Tcherepnin v. Knight*, 389 U.S. 332 (1967); *SEC v. Glenn W. Turner Enterprises, Inc.*, 474 F.2d 476 (9th Cir. 1973); *United Housing Foundation, Inc. v. Forman*, 421 U.S. 837 ("**Forman**"); *International Brotherhood of Teamsters v. Daniel*, 439 U.S. 551 (1979); and *SEC v. Belmont Reid & Co., Inc.*, 794 F.2d 1388 (9th Cir. 1986); and *SEC v. Life Partners, Inc.,* 87 F.3d 536 (1996).

[24] *See, e.g.,* Munchee; Airfox; and *In re Paragon Coin, Inc.*, Securities Act Rel. No. 10574 (Nov. 16, 2018). *See generally SEC v. W.J. Howey*, 328 U.S. 293 (1946).

[25] *SEC v. Kik Interactive Inc.*, Case No. 19-cv-5244, S.D.N.Y, June 4, 2019; *SEC v. Eran Eyal and United Data, Inc. d/b/a "Shopin",* Case No. 19-cv-11325, S.D.N.Y, December 11, 2019; and *SEC v. Telegram Group Inc. and Ton Issuer Inc.*, Case No. 19-cv-9439, S.D.N.Y, October 11, 2019.

In situations where regulators have viewed a native asset to *not* be a security, the underlying blockchain networks have a few features in common: (i) open, but somewhat concentrated, governance,[26] (ii) the perception of widespread mining or voting communities,[27] and (iii) the perception that no single party or small group of persons can exercise Change Control over the protocol's core code. In situations where all three are present, the SEC has not made its *Howey* analysis public and has simply treated the native asset as *not* a security.[28]

We note that in almost all cases, any purchaser of any digital asset "relies on the managerial efforts of others" because those purchasers need other miners, validators, maintainers, et cetera, to ensure the security and stability of the network. Most purchasers of bitcoin, for example, do not mine or host nodes. They rely on the expertise of others to ensure the network stays functional and secure. This sort of "reliance," however, is too attenuated or not attributable to any single or concentrated group of actors to result in bitcoin being considered to be a security.

The sort of "reliance" that draws concern from regulators can be gleaned from reviewing: (i) consent orders and cases involving assets native to blockchain networks and (ii) the regulatory consensus around blockchain-based assets deemed to *not* be securities. Review of both suggests that where a small group of persons[29] commits their expertise to maintaining a network, the SEC will be more likely to find the requisite "reliance" by purchasers.[30] To the contrary, where the network is maintained by a widely distributed and independent group of core developers, the SEC is less likely to treat the native asset as a security.[31] As implied below, where the SEC has made reference to a data point, we treat that data point as relevant to an analysis of political centralization.

When we state a blockchain network is politically centralized, we mean to say, as compared to a Benchmark Network, a relatively small number of persons exercises, and engages in communications with each other regarding network governance or control.

---

[26] *See, e.g.,* Jameson Lopp, *Who Controls Bitcoin Core?* (Dec. 15, 2018), https://blog.lopp.net/who-controls-bitcoin-core-/ ("While Bitcoin Core has some structure (it uses centralized communications channels in order to coordinate), the project itself is not subject to being controlled by any of its participants"); Aaron Van Wirdum, *A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol* (Sep. 7, 2016), https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427 ("Bitcoin Core is governed by a loosely meritocratic process of peer review and rough consensus among its most active contributors."); and Willem-Jan Smits, *Blockchain Governance: What Is It, What Types Are There and How Does It Work in Practice?* (Oct. 24), https://watsonlaw.nl/en/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/ ("Although it is often advertised as being decentralized, the network is still more or less dependent on the input of its founder, Vitalik Buterin, who is in charge of writing the Ethereum code's major changes. Nevertheless, Ethereum uses a similar governance structure to the one of Bitcoin where users can decide on network-wide software alterations by expressing their vote on Ethereum Improvement Proposals (EIPs).").

[27] *See, e.g., Global Bitcoin Nodes Distribution,* Bitnodes (last accessed Feb. 24, 2020), https://bitnodes.io/ (showing that there are 10,869 reachable bitcoin nodes in the network located in at least 97 different countries); and *Ethereum Mainnet Statistics,* Ethernodes (last accessed Feb. 24, 2020), https://www.ethernodes.org/ (showing that there are 7,495 nodes on the Ethereum network located in at least 92 different countries.).

[28] *See supra* note 13.

[29] Note that throughout, we use the term "small group of persons" to refer to natural persons, corporate entities, and organizations. When we wish to refer to living, breathing persons, we use the term "natural persons.".

[30] *See supra* note 25.

[31] *See supra* note 13.

Note on Interactions Between Data Points

Some data points may not reveal any useful information when viewed in isolation. Often, a data point will only be relevant to the extent it raises or lowers the significance of another data point. Sometimes, a data point will be rendered meaningless because another data point's value is too low or too high. Take the data point, Circulation, for example. On its own, it may not reveal much. Even if Circulation shows high distributed circulating supply for an asset, where other indicators show most of that supply lies in the hands of one or two parties, the data point is effectively rendered meaningless. If the distributed circulating supply is low, and the Stake and Release Mechanism data points suggest an influx of a large number of promised tokens, then the fact that circulating supply is low should point anyone investigating economic centralization towards the question of how many network addresses will receive the promised tokens and what economic influence they might wield as a result. Myriad examples can be drawn from deeper analysis of the data points on the list below. We cannot understate the complexity of the web of interactions between seemingly isolated data points. Any analysis regarding these data points should take a consistent view rooted in an understanding of how they interact with each other in the real world.

Note on Potential Data Point Manipulation

We are aware of the risk that data points, generally speaking, may be subject to manipulation by network creators or control persons. While we have not risk rated each data point to determine which among them are more susceptible to manipulation, we do believe that some are very likely to offer high resistance to attempts to manipulate. While this document is an effort to bring objectivity, transparency, and a common taxonomy to the terms "centralization" and "decentralization," we caution that any interested party using a standard dataset comprised of these data points should, first, be aware of any manipulation risk and, second, take steps to prevent or identify such manipulation as part of its due diligence. Over time, we believe certain of these data points may prove to be useful anchors highly resistant to manipulation, or may even be looked to in the first instance to quickly flag obvious attempts at manipulation.

Layer	*"Centralized"*	*"Decentralized"*
Computational	Relative to the Benchmark Networks, fewer nodes send packets of information to each other.	Node activity at least mirrors that of the Benchmark Networks.
Economic	Relative to the Benchmark Networks, fewer network addresses store or transfer significant value.	Significant value transfer activity across network addresses at least mirrors that of the Benchmark Networks.
Political	Relative to the Benchmark Networks, fewer people engage in governance or control decisions.	Diversity of engagement in governance or control decisions at least mirrors that of the Blockchain Networks.

Alphabetical List of Data Points for Measuring Centralization

BLOCK SIZE

COMPUTATIONAL
POLITICAL

The size of the block creates a limit on the number of transactions that can be verified on a blockchain network. Larger blocks require greater computational power and will take longer to be mined. The size of a block is important vis-à-vis other metrics such as Node Communication and Mining Power Concentration (defined below) for the very specific scenario of identifying the risk of selfish mining. Selfish mining was proposed[32] as a strategy for miners to increase their share of overall revenue by hiding newly generated blocks from the main blockchain and creating a separate fork. Selfish miners can strategically time their display of the new blocks such that honest miners abandon their own chain and join the new fork. The result is that "the decentralized nature of the currency will have collapsed, and a single entity, the selfish pool manager, will control the system."[33]

Thus, when a network is at risk of selfish mining, it is also at risk of becoming computationally or politically centralized. Further, larger block sizes may increase the cost of running a full node – where fewer full node operators exist, a network may be more computationally centralized. However, this concern is more directly addressed by the Cost of Running a Node measure listed below.

CIRCULATION

ECONOMIC

Circulation refers to two separate data points: the number of the native asset already distributed and available to transfer and the amount yet to be distributed.[34] These data points can be influenced by a number of things, including (i) a protocol's inflation mechanism, or the rate at which new native assets get distributed, and (ii) the percentage of the native asset lost, locked, or burned ("**Loss Percentage**").

Understanding how far circulating supply is from reaching its maximum distribution limit, considering both the inflation mechanism and the Loss Percentage, may be helpful when considering economic control over a network. The data points on their own do not provide special insight into economic centralization. We include them here because, when considered in conjunction with other data points (e.g., Stake and Release Mechanism, defined below), they affect their importance.

---

[32] Eyal et al, *Majority is not Enough: Bitcoin Mining is Vulnerable*∗ (Nov. 1, 2013), https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf.

[33] *Id.*

[34] *See e.g.,* Coin Metrics' State of the Network, *Coin Metrics' State of the Network: Issue 26* (Nov. 19, 2019), https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e?.

CLIENT SOFTWARE

COMPUTATIONAL
POLITICAL

A blockchain wallet generates and stores private keys.[35] The term "wallet," however, is often used to refer to the software that stores private and public keys and interacts with various blockchains to enable users to send and receive digital currency and monitor their balance.[36] A "client" is the software responsible for the generation of private keys and transaction construction, making it the apparatus by which a user interacts with the blockchain.

Availability

Some blockchains might only have one client developed by a private company which launched the network or ran a related token sale. Others might have many open source, third party clients. The number of client software choices available to an end user, and the nature of those clients can speak to the centralization of a network. Participants on the blockchain network may find themselves reliant on the expertise of a small number of developers to develop and maintain client software, which would speak to political centralization (especially if these options are not open source).

Popularity

Following the point above, even where many options exist with respect to client software, in practice the use of one client software has dominated.[37] A network with a popular client may present a point of failure; if nodes devoted to maintaining the network primarily use that client, this would speak to computational centralization.[38]

COMPENSATION

ECONOMIC
POLITICAL

Some projects will build into the distribution protocol a funding release that rewards or compensates developers, foundation members, or employees with the native asset prior to the native asset having any value.[39] Such compensation incentivizes both political and economic

---

[35] Blockchain, *Public and Private Keys* (May 17, 2020), https://support.blockchain.com/hc/en-us/articles/360000951966-Public-and-private-keys.

[36] Ameer Rosic, *Cryptocurrency Wallet Guide: A Step-By-Step Tutorial* (2017), https://blockgeeks.com/guides/cryptocurrency-wallet-guide/.

[37] See William Foxley, *Ethereum Developers Delay Berlin Hard Fork to Stem Client Centralization Concerns (June 30, 2020)*, https://www.coindesk.com/ethereum-developers-delay-berlin-hard-fork-to-stem-client-centralization-concerns (Geth makes up only one of 11 client specifications, but 79% of Ethereum nodes run on it. That percentage is also up 5% since December. Developers worry that a serious bug could break Ethereum …).

[38] *See, e.g.,* Christine Kim, Bitcoin Cash's Scheduled Hard Fork Tripped Up By Software Bug (May 15, 2019), https://www.coindesk.com/bitcoin-cash-scheduled-hard-fork-tripped-up-by-software-bug ("Having a single type of node is a form of centralization – you're trusting the codebase from the node type you've selected to keep working as expected."). *See also* American Crypto Association, *Is Satoshi Nakamoto Being Proven Right About Multiple Clients* (Feb. 21, 2020), https://www.americancryptoassociation.com/2020/02/21/is-satoshi-nakamoto-being-proven-right-about-multiple-clients/ (noting that the best argument for multiple clients is that "if one has a bug and the other doesn't, then the network can still keep running.").

[39] *See, e.g.,* Zooko Wilcox, *Funding, Incentives, and Governance* (Sep. 23, 2019), https://electriccoin.co/blog/funding/.

activity that steers the network in a manner that suggests centralization. For instance, compensation that is denominated in the native asset at a project's outset may motivate a small number of persons to promote the network in a way that increases the value of the asset, a concern noted by the SEC as important to the "reliance" analysis.[40] Additionally, compensation schemes to developers involving freely transferable native assets may present a moral hazard in the form of a motivation to engage in insider trading.

CONCENTRATION OF ACTIVITY AMONG CODE CONTRIBUTORS

POLITICAL

A high concentration of activity among code contributors – whether on GitHub or another developer platform – may indicate reliance on the efforts and expertise of a small number of persons for the ongoing maintenance of the network, relevant to an analysis of political centralization. The reliance is made apparent where developers or their employees have explicit responsibility to maintain the network.[41]

COST OF RUNNING A NODE

COMPUTATIONAL

The level of censorship resistance and resilience of a blockchain network depends in part on how many nodes run at any given time. Thus, the financial cost of running a node is important in understanding computational centralization. The greater the expense of running node, the less likely many global actors can run one. Factors affecting cost include energy price, disk space required, internet access price, mining rig expense, block rewards (i.e., native assets rewarded to miners upon successful validation of a new block), and the native asset's price.[42]

EXCHANGE LISTINGS

ECONOMIC

This data point references the *number* of exchanges a native asset is listed on as well as the *variety and type* of exchange. Some exchanges claiming to be "decentralized" allow for global access with minimal to no onboarding due diligence. Others may be restricted to certain countries or to wealthy individuals. A native asset may generally find itself in one of three camps – widely traded on a range of centralized and "decentralized" exchanges (or trading desks), only available on "decentralized" exchanges with thin volume (as compared to assets on centralized exchanges), or not available on any exchanges (or trading desks). In any event, for native assets at the margins of listing availability, access to decentralized exchanges may increase the overall availability of native asset trading. All else being equal, a native asset with fewer listings will likely

---

[40] *See* SEC Framework at 5 (indicating an increased likelihood that the purchaser of the digital asset is relying on the efforts of others when the "AP distributes the digital asset as compensation to management or the AP's compensation is tied to the price of the digital asset in the secondary market. To the extent these facts are present, the compensated individuals can be expected to take steps to build the value of the digital asset.").

[41] *See, e.g.,* The Core Team, *An update from the Core Team on some technical responsibilities* (Dec. 16, 2019), https://web.getmonero.org/2019/12/16/technical-responsibilities-update.html.

[42] *See* Josiah Wilmoth, *Bitcoin Miners are Selling Old ASICs for Scrap Metal as Price Decline Hastens Obsolescence* (Nov. 23, 2018), https://www.ccn.com/bitcoin-miners-are-selling-old-asics-for-scrap-metal-as-price-decline-hastens-obsolescence/.

have a smaller number of network addresses transferring value on the economic layer (barring the exceptional circumstance of an asset native to an exchange).

EXISTENCE OF KEY INFLUENCERS

ECONOMIC
POLITICAL

A key influencer is a person (including blockchain development companies or similar organizations) with a community following or an established and trusted reputation for representing a specific blockchain network. Such influencers may exert control and influence over the decisions of others regarding the project, whether via social media, control over websites, social media handles, exercise of intellectual property ("**IP**") controls, sponsorships, or through their role as a spokesperson. An influencer's unilateral ability to increase demand, raise awareness, encourage value transfer, or influence key governance decisions on a regular basis may be relevant to either the political or economic datasets regarding centralization.

GITHUB PROJECT STATISTICS

POLITICAL

GitHub project statistics can indicate how active developers are with respect to a network. They can also provide a sense of overall popularity of the network and a view into the volume of developer work committed to date.[43] Standing alone, this data point does not speak to the likelihood of centralization of Voting Control or Change Control. However, when combined with the Concentration of Activity Among Contributors and Number of Contributors data point, it can shed light on whether there exists reliance on a small number of persons for the ongoing maintenance of the network.

GOVERNANCE

POLITICAL

Development Efforts, Network Control, and Updates

Governance mechanisms vary across projects. Governance can be conducted on-chain or off-chain (or a combination of both), voting may be restricted to certain issues put forth by maintainers, the proposal submission process may be tightly controlled, or a board or foundation might exercise significant influence over protocol changes. Many regimes prevent critical decisions from being made by a small group of persons.

Where governance over development efforts, network control, and updates to the protocol's core code occurs among a small group of persons, and even where decisions may be subject to a community vote, such limited control or control over proposals may

[43] *See, e.g.,* Charlie Lee (@SatoshiLite), Twitter (Aug. 11, 2019, 2.21 AM), https://twitter.com/SatoshiLite/status/1160436027099451392 ("4/ Recently there's been a lot of FUD about Litecoin having no code commits in 2019. When you look at Litecoin GitHub (https://github.com/litecoin-project/litecoin), it would seem like we did no work in 2019.").

lead to the sort of "reliance" relevant to the SEC.[44] Examples of relevant controls include control over kill switches,[45] control over oracles important to a protocol,[46] backdoors,[47] wallet whitelisting,[48] and the ability to remove projects from the network.[49]

A combination of governance controls and lack of participation may result in de facto influence over a protocol. Taking the less common example of blockchain-based, explicit and binding voting as illustrative: where a small group of persons holds a majority of a native asset or voting power,[50] unique voter turnout is consistently low, and votes are weighted according to the amount of the asset a voter holds, decisions can effectively be made by a small group of persons. While certain governance designs may attempt to prevent such undue voting influence, for example by implementing one vote per person rules, or ensuring all decisions can be put up for voting, the more common scenario for blockchain governance is one of informal, structureless governance. Such structures may leave a range of interested parties without explicit voting power (e.g., miners) with opportunities to exercise de facto control over a network.

---

[44] *See* SEC Framework at 4 (indicating an increased likelihood that the purchaser of the digital asset is relying on the efforts of others when "AP has a lead or central role in the direction of the ongoing development of the network or the digital asset. In particular, an AP plays a lead or central role in deciding governance issues, code updates, or how third parties participate in the validation of transactions that occur with respect to the digital asset.").

[45] *See, e.g.,* Augur Project, *Augur Weekly Update – July 2th,* Medium (Jul. 26, 2018), https://medium.com/@AugurProject/augur-weekly-update-july-25th-b49e2771af9a ("Additionally, ownership of the escape hatch contract has been transferred to a burn address.").

[46] *See, e.g.,* Ryan Todd, *Synthetix suffers oracle attack, more than 37 million synthetic ether exposed* (Jun. 24, 2019), https://www.theblockcrypto.com/linked/28748/synthetix-suffers-oracle-attack-potentially-looting-37-million-synthetic-ether.

[47] *See, e.g.,* Jeremy Kirk, *Exclusive: Aussie Firm Loses $6.6M to Backdoored Cryptocurrency* (June 5, 2018), https://www.bankinfosecurity.com/exclusive-aussie-firm-loses-5m-to-backdoored-cryptocurrency-a-11057 (explaining that the backdoor allowed an account owner to call a particular function and transfer a balance from anybody to anybody.).

[48] *See, e.g.,* Tim Fries, TokenSoft CEO Explains Security Token Whitelisting (Sep. 15, 2020), https://thetokenist.io/tokensoft-ceo-explains-security-token-whitelisting/#:~:text=One%20aspect%20of%20compliant%20security,which%20represents%20authorized%20token%20holders ("Whitelisting allows for the issuer to ensure— through smart contract management— that only approved addresses can receive the tokenized asset … ").

[49] *See, e.g.,* Valerian Bennett, *Banned from the Blockchain: An Ethereum developer's tale of migrating to TRON,* Medium (Dec. 24, 2019), https://medium.com/popnetwork/banned-from-the-blockchain-an-ethereum-developers-tale-of-migrating-to-tron-248a0d215c92.

[50] *See, e.g.,* Daniel Phillips et al, *Curve founder seizes 71% of Curve DAO voting power* (Aug. 23, 2020), https://decrypt.co/39599/curve-founder-seizes-71-of-curve-dao-voting-power.

Funds Deployment

Some projects maintain a project-specific pool, replete with the native asset, from which efforts to develop the network will be funded.[51] The existence of such a fund to service, improve, maintain, market, spread awareness of a network has been deemed indicative of the "reliance" relevant to the SEC.[52] The potential for such "reliance" becomes amplified where the same parties in control of fund governance also possess relevant IP controls or a company pays employees in the native asset to further develop the network.[53]

INTELLECTUAL PROPERTY

POLITICAL

IP refers to intangible assets owned and subject to legal rights enforceable by a company, and includes patents, copyrights, and trademarks. Companies that publish via an open source license may maintain some IP rights over the code.

Where IP rights exist, they can allow a company to prevent use of the name of a blockchain network or its native asset,[54] or to prevent use of the code for purposes such as hard-forking.[55] The existence of such IP rights may indicate participants are likely to rely on the efforts of a small group of persons to ensure the protocol's core code is protected from hard forks that may divert value away from their network and the native asset. By possessing legal protections over IP and threatening to enforce them, the IP owner can attempt to limit the behavior of independent developers wishing to change the network.[56]

---

[51] *See, e.g.,* Michael McSweeney, Pseudonymous SushiSwap founder returns 38,000 ETH to project treasury after public outcry (Sep. 11, 2020), https://www.theblockcrypto.com/linked/77587/sushiswap-founder-eth-project-treasury; and Uniswap, *Introducing UNI* (Sep. 16, 2020), https://uniswap.org/blog/uni/ ("1 billion UNI have been minted at genesis and will become accessible over the course of 4 years. The initial four year allocation is as follows: … 21.51% to team members and future employees with 4-year vesting").

[52] *See* SEC Framework at 7 (indicating an increased likelihood that there is a reasonable expectation of profit where the AP continues to expend funds from proceeds or operations to enhance functionality or value of the network or digital asset or to market it. Additionally, any public indication that the company will operate, promote, improve or otherwise continue to work on network developments would be indicia of the existence of a "reasonable expectation of profits.").

[53] *See* SEC Framework at 5 (indicating an increased likelihood that the purchaser of the digital asset is relying on the efforts of others when the AP owns or controls ownership of intellectual property rights of the network or digital asset, and when the AP distributes the digital asset as compensation to management.). *See also* Uniswap, *Introducing UNI* (Sep. 16, 2020), https://uniswap.org/blog/uni/.

[54] *See, e.g., Zcash Foundation Guidance on Dev Fund Proposals,* Zcash Foundation (Aug. 6, 2019), https://www.zfnd.org/blog/dev-fund-guidance-and-timeline/ ("From a legal perspective, the Zcash trademark is currently enforced, protected, and owned by ECC. As things stand today, ECC has the authority to decide what products and services can legally be labeled Zcash.").

[55] *See, e.g.,* Mochimo Cryptocurrency Engine License Agreement Version 1.0, *available at* https://github.com/mochimodev/mochimo/blob/master/LICENSE.PDF (last accessed Apr. 26, 2020) (granting the right to any contributor to modify the source code of the Mochimo Cryptocurrency Engine only "to improve or change the behavior of the Mochimo cryptocurrency and the Mochimo cryptocurrency network and for no other purposes …").

[56] See supra note 55.

ISSUER INFLUENCE OVER EXCHANGE LISTINGS

POLITICAL

Some developers or their affiliates who issue the native asset ("**Issuers**") may attempt to exercise influence over cryptocurrency exchanges wishing to list those assets. Alternatively, cryptocurrency exchanges may look to the Issuers to provide technical or security related support when listing a new native asset.[57] Successful exercise of such influence may indicate that participants on the blockchain network for that native asset rely on the listing efforts of Issuers to see a profit, a relevant consideration for the SEC.[58]

LIQUIDITY PROVISION

ECONOMIC
POLITICAL

Liquidity mechanisms include buybacks, airdrops, giveaways, issuance of more tokens. Liquidity providers, such as market makers, generally consist of persons ready to purchase or sell a native asset at a given price, usually for the purposes of providing liquidity to meet organic market demand, reduce volatility on an exchange, or aiding with price discovery.

Issuers may announce plans to provide liquidity to a new network, may engage in providing such liquidity, or may hire market makers to provide such liquidity. The SEC has indicated that such liquidity provision is problematic for the "reliance" analysis.[59] This data point may also be important to an analysis of economic centralization as liquidity plans may result in a greater number of network addresses interacting with each other. Depending on the facts and circumstances, the network addresses of some liquidity providers, such as those sponsored by an Issuer, may have a limited impact on the analysis of either economic or political centralization.

MARKET ATTACK COST

ECONOMIC

The market attack cost is the cost of causing the market price of a native asset to reduce to zero, close to zero, or to cause a material percentage decrease in price ("**Price Crash**"). Where it is relatively inexpensive to cause a Price Crash on secondary markets, this may be a result of the existence of a derivatives market, low liquidity, low market depth, or the ease with which persons can otherwise manipulate the market. Such a market may be susceptible to influence by a small number of network addresses possessing controlling amounts of a native asset.

---

[57] *See, e.g.,* Trust Nodes, Sushi Chef Deletes Private Conversation with Coinbase Listing (Sep. 2, 2020), https://www.trustnodes.com/2020/09/02/sushi-chef-deletes-private-conversation-with-coinbase-listing.

[58] See *Munchee*; *Airfox*; and SEC Framework at 4 (risk factor where a central party has "arranged, or promised to arrange for, the trading of the digital asset on a secondary market or platform.").

[59] *See* SEC Framework at 4 (indicating an increased likelihood that the purchaser of a digital asset is relying on the efforts of others when the AP creates or supports a market for, or the price of, the digital asset by, for example, controlling the creation and issuance of the digital asset, limiting supply or ensuring scarcity through buybacks or "burning".)

MINING POWER CONCENTRATION

COMPUTATIONAL
ECONOMIC
POLITICAL

Mining power concentration refers to how much of the computing power dedicated to securing an underlying blockchain network is concentrated among nodes, network addresses, or persons. The data point can also be referred to as "Hash power Concentration."

Where the concentration of mining power is high,[60] the risk of collusion[61] or shutdown from external forces such as government pressure[62] or environmental disasters[63] is greater. These risks highlight that a network may be subject to centralization at any layer – computational, economic, or political.[64] The network may also be susceptible to a network attack where the controllers of the majority of the hash power could potentially reverse transactions, prevent confirmation of new transactions and conduct double spends.

NETWORK ATTACK COST

COMPUTATIONAL
POLITICAL

The network attack cost is the amount of resources (monetary or non-monetary) it would take to successfully attack the network.[65] Resources may include hardware or purchased hashing power. Historically, most believed the risk of network attack was low due to the extremely high costs required to successfully execute such an attack.[66] New blockchain networks have low hash power

---

[60] *See, e.g.,* Tom Wilson, *China's bitcoin miners scoop up greater production power -research* (Dec. 11, 2019), https://www.reuters.com/article/us-crypto-currencies-mining/chinas-bitcoin-miners-scoop-up-greater-production-power-research-idUSKBN1YF1PB ("Miners in China control 66% of global "hashrate" … according to a report by digital asset manager CoinShares.").

[61] *See, e.g.,* Rachel McIntosh, *2 Bitcoin Cash Mining Pools Organized 51% Attack to Thwart Hacker* (May 27, 2020), https://www.financemagnates.com/cryptocurrency/news/2-bitcoin-cash-mining-pools-organized-51-attack-to-thwart-hacker/.

[62] *See* Paul Muir, *Dry season offensive against China bitcoin miners* (Dec. 29, 2019), https://www.asiatimes.com/2019/12/article/dry-season-offensive-against-china-bitcoin-miners/ ("Regional authorities in the province of Sichuan are reportedly pressuring bitcoin miners to scale down operations amid electricity shortages during the dry season in southwest China.").

[63] *See, e.g.,* Wolfie Zhao, *Top Bitcoin Mining Pools See 15% Hashrate Drop Amid Continuous Rainstorms in China* (Aug. 18, 2020), https://www.coindesk.com/bitcoin-mining-hash-rate-rainstorms-china ("Major Chinese bitcoin mining pools are each seeing daily hashrate drops of between 10% and 20% following continuous rainstorms in Sichuan … The computing power connected to these four pools accounts for around 50% of the Bitcoin network's total.").

[64] *See, e.g.,* Danny Nelson, *BitGo is processing more than 20 percent of bitcoin transactions, the company said at CoinDesk's Invest: NYC conference today* (Nov. 12, 2019) https://www.coindesk.com/bitgo-says-its-now-processing-20-of-bitcoin-transactions ("It also raises questions about market collapse: If BitGo goes down, would those assets be at risk?").

[65] *See, e.g., PoW 51% Attack Cost,* Crypto51, https://www.crypto51.app/ (last visited Dec. 20, 2019) (Showing how expensive it is to 51% attack various blockchains using a mining marketplace.); and *Hash power Marketplace*, Nicehash, https://www.nicehash.com/marketplace/ (last visited Dec. 20, 2010) ("NiceHash enables you to buy hashing power from other people.").

[66] *See* Rodd Garratt and Rosa Hayes, *Bitcoin: How Likely Is a 51 Percent Attack?* (Nov. 24, 2014), https://libertystreeteconomics.newyorkfed.org/2014/11/bitcoin-how-likely-is-a-51-percent-attack.html ("Is there a one-

compared to more established networks, making such attacks no longer theoretical. Since 2018, there have been a growing number of double spend attacks.[67] Where the cost of attacking a network is low and the level of expertise required to do so is not high, computational centralization remains a risk. Low network attack cost also presents the risk that small groups of persons have the ability to exclude or modify the ordering of transactions, prevent transactions from being confirmed or conducting double spends.

NETWORK COMPLETION

POLITICAL

Because blockchain networks can be modified over time, some launch without all of their publicly promised features. Such networks may be deemed "incomplete" even if they have attained a level of functionality. A project that touts that it is "incomplete" and has improvements pending may signal to the general public that participants must continue to rely on a small group of persons to "complete" the network. Such promises have been indicative of "reliance" by the SEC.[68] Note, however, a network may be incomplete and still be "mature," depending on the SEC's ultimate view of "network maturity." What is relevant to the SEC is whether marketing materials leave purchasers with an expectation they must rely on a small group of people to see value in the asset they purchased.

NODE COMMUNICATION

COMPUTATIONAL

Node communication is composed of the speed and distance with which a transaction propagates through the network, the discovery and connection method between nodes, the mechanism of relaying information between nodes, and the content each node receives and validates. For some networks, all full nodes validate all transactions.[69] On others, nodes might validate a small section of a block is related to the node without verifying the actual transaction content. The differences here may not be relevant when viewed in isolation, but may inform other data points relevant to computational centralization. For instance, node communication methods may make concentration or geographic distance between nodes more or less relevant depending on the context.

---

shot manipulation that will earn the controlling mining pool more than its expected future earnings? If not, then the pool has little incentive to manipulate the blockchain, as doing so would destroy its source of future income.").

[67] *See, e.g.,* Alyssa Hertig, *Blockchain's Once-Feared 51% Attack Is Now Becoming Regular* (Jun. 8, 2018), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular; and Zack Voell, *Ethereum Classic Attacker Successfully Double-Spends $1.68M in Second Attack: Report* (Aug 7, 2020), https://www.coindesk.com/ethereum-classic-attacker-successfully-double-spends-1-68m-in-second-attack-report.

[68] *See* SEC Framework at 3 (indicating an increased likelihood that the purchaser of a digital asset is relying on the efforts of others when the network or the digital asset is still in development and the network is not yet fully functional at the time of the offer or sale.).

[69] *See, e.g.,* Bitcoin Wiki, *Satoshi Client Block Exchange* (Jan. 18, 2013), https://en.bitcoin.it/wiki/Satoshi_Client_Block_Exchange.

NODE CONCENTRATION

COMPUTATIONAL
POLITICAL

A node is a physical computer operating the software required to bring about the existence of a blockchain network. This data point measures how physically close nodes are with respect to each other.

Where nodes are physically located close to each other, they are exposed to a single point of failure whether it be as a result of (i) being controlled by a person, company or organization (a concern better measured by Mining Power Concentration); or (ii) being susceptible to damage caused by natural disasters, fire, flood, or physical intervention such as confiscation by local authorities[70] or theft of mining rigs.[71] The latter situation could cause failure of a substantial part of the network's nodes, assuming high levels of concentration. As a result, where greater concentration exists, computational centralization is more likely to exist. Increased risk of political centralization logically follows, as a small group of persons will likely control highly concentrated nodes.

NUMBER OF CONTRIBUTORS

POLITICAL

A contributor is anyone who contributes to coding, reviewing, testing, translating, or documenting the project. Contributors are essential to governance, maintenance, and ongoing operation of the network. A small number of active contributors that initially create and deploy the network indicates a likelihood that network participants will rely on the managerial efforts and expertise of that small group of persons.[72] However, contributor count may be less relevant on balance when Voting Control or Change Control is highly centralized.

---

[70] *See, e.g.,* Ana Alexandre, *Chinese Authorities Confiscate Nearly 7,000 Crypto Mining Machines (Dec. 23, 2019),* https://cointelegraph.com/news/chinese-authorities-confiscate-nearly-7-000-crypto-mining-machines ("The cryptocurrency mining confiscation came as part of an inspection of more than 70,000 households, 3,061 merchants, 1,470 communities, as well as factories, mines, courtyards and villages in the Kaiping District of Tangshan city.").

[71] *See, e.g.,* Jamie Redman, *Iceland's 'Big Bitcoin Heist': Suspects Charged With Over $2M in Stolen Mining Rigs* (Sep. 10, 2018), https://news.bitcoin.com/icelands-bitcoin-heist-suspects-charged-with-over-2m-in-stolen-mining-rigs/.

[72] *See, e.g.,* Charlie Lee (@SatoshiLite), Twitter (Aug. 11, 2019, 2.21 AM), https://twitter.com/SatoshiLite/status/1160436034359791617 ("... we've only had a handful of core developers working on Litecoin Core … Since we are mostly just merging in Bitcoin changes, we only need a lead Litecoin Core developer doing the merges and the rest of us help with code reviews, testing, and gitian builds."); and TrustNodes, *"No One is Interested in Working on Litecoin" Says Charlie Lee* (Aug. 11, 2019), https://www.trustnodes.com/2019/08/11/no-one-is-interested-in-working-on-litecoin-says-charlie-lee.

NUMBER OF MAINTAINERS

POLITICAL

Maintainers (or code editors) are persons who either have commit access or rights to accept software changes to the protocol's core code and are responsible for pull requests from contributors. Pull requests are a series of changes submitted by developers for review by the maintainer. Maintainers act as a final check to ensure pull requests are safe and in line with a project's goals. Lead maintainers are responsible for the release cycle, overall merging, moderation, and appointment of maintainers.

Because a maintainer's role is essential in effecting and ultimately deciding which changes are put up to the network for voting, where a small number of maintainers curate such proposals, this indicates the network's continued reliance on the expertise and efforts of a small group of persons. The level of dependency on and control by the maintainers may depend on the governance process for selecting new maintainers and the amount of filtering conducted by the maintainers. For example, where new maintainers can only be chosen by existing or lead maintainers, where maintainers are selective in accepting changes and are effectively deciding which changes can receive votes, it is evident key decisions are being executed by a small group of persons. In short, vote curation activity is relevant to the *Howey* analysis.[73] Furthermore, if a lead maintainer is the only active maintainer doing the work, the ongoing maintenance of the network might be almost solely dependent on that maintainer, indicating a higher risk of political centralization.[74]

NUMBER OF NODES

COMPUTATIONAL

A node is a computer or electronic device running software. Nodes maintain either a full or partial copy of the blockchain and employ computing power to confirm transactions through a consensus protocol. There are different types of nodes with different functionalities that may vary depending on the consensus mechanism and underlying protocol.

Full Nodes

Full nodes keep its own copy of the blockchain and can use that copy to validate all transactions and blocks.[75] If a full node validates a transaction or block, it relays that data to other full nodes so that they can come to a consensus. Full nodes also ensure that the transactions have been executed according to the rules of the protocol. The greater number of full nodes, the more computationally decentralized and resistant the network becomes to certain attacks. Full nodes may be validator nodes or non-validator nodes.

---

[73] SEC Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, SEC Release No. 81207 (July 25, 2017) at 12-15 (mentioning Curator control and limited voting power as indicia of reliance on the efforts of others).

[74] *See, e.g.,* Paddy Baker, *Monero's 'Fluffypony' Steps Down as Lead Maintainer of Privacy Coin Project* (Dec. 18 2019), https://www.coindesk.com/moneros-fluffypony-steps-down-as-lead-maintainer-of-privacy-coin-project ("I'm stepping back as lead maintainer but continuing on as a maintainer, to further decentralize the project").

[75] Lightweight nodes perform a similar function to full nodes but only contain a portion of the blockchain. They only download the block header of previous transactions, to confirm the validity of the blockchain, and to pass this information on to other nodes.

In the specific context of proof of stake networks (or certain other blockchains), the term "master node" may appear as a stand-in for the term "full node."

Validators

A validating node communicates with other nodes in the network to receive and relay transactions, ensuring that each does not violate the transaction rules. Where few validating nodes exist, participants may be reliant on a small number of nodes for maintenance of the network, as well as for reliable transmission and validation of transactions. In the event that validating nodes fail concurrently, the network may cease to work as designed and be susceptible to various attacks or failures.[76]

PERMISSIVE LICENSING

COMPUTATIONAL
POLITICAL

A blockchain network is said to be fork-able where the source code has been published under a free and open source software ("**FOSS**") license, also known as permissive licenses. Such networks can have the original source code altered by any persons but require hash power or community support to effectively migrate participants from the original source code to the modified one. Generally, FOSS code allows anyone who disagrees with a blockchain network's design to rewrite the protocol's core code and attempt to launch a new, modified version of the network.

The open source nature of code can indicate the lack of a central point of Change Control over the protocol's core code, although this indication can be rebutted by looking to governance design and intellectual property controls. In addition, the existence of coordinators[77] as well as attempts to coordinate hard forks,[78] upgrades, or bug fixes would rebut any indication that the open source nature of the code actually indicates the lack of a central point of Change Control.

POTENTIAL TO ACCESS MNPI

POLITICAL

Material non-public information ("**MNPI**") in the context of a blockchain network may include, among other things, technical information (e.g. a catastrophic bug in the source code, impending upgrades), market related information (e.g. impending listing on an exchange, details of an upcoming burn or market dump), or governance information (e.g. switching from centralized control to a decentralized voting system). Individuals privy to MNPI may have access because

---

[76] *See, e.g.,* Stellar Development Foundation, *May 15th Network Halt, Stellar Developers* (May 16, 2019), https://medium.com/stellar-developers-blog/may-15th-network-halt-a7b933103984 ("The outage on May 15 left the Stellar network in a fragile state, with only 4 parties as the core validators … The network was taken down briefly while we repaired this.").

[77] *See, e.g.,* James Hancock (@JHancock), Twitter (last accessed Dec. 24, 2019), https://twitter.com/JHancock (Referring to himself as a "HardFork Coordinator" in his biography).

[78] *See, e.g.,* Ethereum, *Ethereum Core Devs Meeting 68 Notes,* GitHub (Aug. 18, 2019, 22:00 UTC), https://github.com/ethereum/pm/blob/master/All%20Core%20Devs%20Meetings/Meeting%2068.md; and *Ethereum Developers Unanimously Agree to Delay the Difficulty Bomb,* Trustnodes (Nov. 30, 2019) https://www.trustnodes.com/2019/11/30/ethereum-developers-unanimously-agree-to-delay-the-difficulty-bomb.

they control websites or forums, have exclusive access to bug reports,[79] procure listing on exchanges, or coordinate proposed changes to the network. MNPI ceases to be non-public once a development team discloses it publicly.

Political centralization is likely to exist where: (1) MNPI exists; (2) only certain people have access to this MNPI due to their position and they choose to keep the information to themselves; (3) some with access to the information, prior to its public release, act or refrain from action based on knowledge of the information.[80] In the scenario above, economic or computational activity may rely on political activity underlying the network. For example, a small number of persons may be responsible for ensuring bugs are fixed and mining pools have updated their software before bugs can be exploited or an unintentional hard fork occurs. If those bugs are not fixed, economic or computational activity may be critically affected.

RELEASE MECHANISM

The release mechanism refers to the rate at which predetermined native asset distribution occurs, whether such distribution occurs via a premine or a postmine. The release mechanism may be enforced by "locking" of a native asset (especially in the premine scenario) subject to certain time limits or milestones. A release mechanism can be designed to dampen the market price influence of premine or postmine recipients. However, a release mechanism may also be perpetual in a manner that ensures continued control over the market price by a small number of network addresses or persons.[81] This data point can thus affect the importance of a premine or a postmine when considering economic or political centralization.

---

[79] *See, e.g., Contribute Bug Reports*, Bitcoin Core (last accessed Dec. 30, 2019), https://bitcoin.org/en/bitcoin-core/contribute/issues.

[80] These three conditions have existed with respect to blockchain protocols in the past. *See* Alyssa Hertig, *The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret* (Sep. 21, 2018), https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret ("Because of the disastrous implications of the bug, developers decided to keep it a secret, buying themselves time to fix the exploit and urge miners and users to upgrade their software."); and *CVE-2018-17144 Full Disclosure,* Bitcoin Core (Aug. 20, 2018), https://bitcoincore.org/en/2018/09/20/notice/ (explaining that "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.").

[81] *See, e.g., ECC Response to Zcash Community Polling Results, Electric Coin Co.* (Dec. 5, 2019), https://electriccoin.co/blog/ecc-response-to-zcash-community-polling-results/ ("The Zcash Community is in favor of continuing to fund Zcash development …").

STAKE

ECONOMIC
POLITICAL

A person's stake, or holdings, in a blockchain network refers to the quantity of a native asset controlled by their private keys. The percentage of these holdings as compared to the entire set of tokens or coins in circulation, indicates the degree of network ownership or influence one entity may have. This data point becomes relevant when assessing the stake or holdings of founding members and initial investors who hold a significant portion of the token supply. The number of the native assets custodied or owned by a person is also politically relevant in networks with on-chain voting or staking mechanisms.

A higher ratio of holdings to circulating supply among few individuals suggests more centralization, while more distributed stake and lower ratios across the network suggests the opposite. Note that any measure of stake should also take into account postmine or premine distribution, and percent held by the largest holders or in exchange wallets (see below).[82]

Postmine Distribution

A postmine generally refers to a pre-assigned, automated distribution of a native asset to specific network addresses after network launch. Where a small number of persons obtain rights to a significant postmine amount, most of the native asset's supply may rest under the control of a small number of network addresses after network launch. Such arrangements may indicate economic centralization and may also indicate "reliance" on the efforts of those controlling these addresses to see value increase.[83]

Premine Distribution

A premine can either refer to the ability to access mining software prior to public release, or to the distribution of a number of native assets before the public has access to the underlying protocol. As with a postmine, where a small number of persons access a significant premine amount prior to public release, most of the native asset's supply may be under the control of small number of network addresses at the time of network launch. Such arrangements may indicate economic centralization and may also indicate "reliance" on the efforts of those controlling these addresses to see value increase.[84]

---

[82] *See, e.g.,* Nicholas Gans, *STEEM Community Battles for Control* (Mar. 5, 2020), https://medium.com/incas/steem-community-battles-for-control-3b751cebb01b ("A large percentage of the STEEM & STEEM POWER assets were held by Steemit Inc at the time of Sun's acquisition, most of which came from the coin's pre-mine (called the "ninja-mined stake"). This now became controlled by Justin Sun, even though the funds were said to be used only for decentralizing and developing the ecosystem.").

[83] *See* SEC Framework at 5 (indicating increased likelihood that purchasers of digital assets are relying on the efforts of others where the AP retains a stake or interest in the digital asset.).

[84] *Id.*

Percent Held By Largest Holders

Some network addresses may have a high percentage of a native asset's circulating supply in their possession. Such concentration indicates economic centralization, and may also indicate political centralization – to the extent holders of the native asset "rely" on the efforts of these large holders to maintain value in their investment.[85] Such concentration may also mean a small group of persons has a significant amount of Voting Control or Change Control.

Percent in Exchange Wallets

Some exchanges may have a high percentage of a native asset's circulating supply in their possession. Such concentration may place the market price at risk of influence by a small number of network addresses and persons, whether those persons are within the exchange (i.e., internal theft, cybersecurity failures, operational failures leading to shutdown) or external to it (i.e., theft, hacks). Such a scenario can indicate economic or political centralization. Further, depending on the facts and circumstances, a high percentage of a native asset under the control of a small number of persons can be problematic under *Howey*.[86]

[85] *See* SEC Framework at 5 (indicating increased likelihood that purchasers of digital assets are relying on the efforts of others where the AP has the ability to realize capital appreciation from the value of the digital asset.).

[86] *See* supra note 83.

Table of Relevant Data Points

COMPUTATIONAL	ECONOMIC	POLITICAL
Block Size	Circulation	Block Size
Client Software	Compensation	Client Software
Profitability of Running a Node	Exchange Listings	Compensation
Mining Power Concentration	Existence of Key Influencers	Concentration of Activity Among Code Contributors
Network Attack Cost	Liquidity Provision	Existence of Key Influencers
Node Communication	Market Attack Cost	GitHub Project Statistics
Node Concentration	Mining Power Concentration	Governance
Number of Nodes	Release Mechanism	Intellectual Property
Permissive Licensing	Stake	Issuer Influence Over Exchange Listings
		Liquidity Provision
		Mining Power Concentration
		Network Attack Cost
		Network Completion
		Node Concentration
		Number of Contributors
		Number of Maintainers
		Permissive Licensing
		Potential to Access MNPI
		Release Mechanism
		Stake

Alphabetical List of Data Points Not Measured

In addition to the data points above, we considered the data points listed below but do not suggest including them as additional values to measure "centralization." We discuss our rationale in detail in this section.

ANONYMOUS FOUNDERS OR DEVELOPERS

The inability to identify founders or developers of a protocol may make it difficult to change or shut down the network or to bring enforcement proceedings against in the event of violations, even where the network is highly centralized.[87] This may give the illusion of a decentralized network because (1) it is not clear whether there are a few individuals or a large group of people running the network;[88] and (2) it is not possible to target them if there was a desire to shut down or control the network.

However, anonymity on its own is not a reliable indicator of network centralization. For example, one anonymous person can theoretically hold the technical ability to maintain and control the network, or a thousand anonymous persons can. We see no reliable causation or correlation between anonymity and centralization.

BLOCKCHAIN SIZE

The size of a blockchain is dependent on a number of factors, including age, usage, and block size, but it cannot be a reliable indicator of a network's centralization. Large blockchains may be centralized, and small blockchains may not be. There exists no meaningful connection between a blockchain's size and network centralization.

CONCENTRATION OF USERS

Where a large portion of a network's users are clustered within a certain jurisdiction or region, certain external events (such as environmental disasters, internet firewalls, or regulatory actions) may remove an entire user base. However, a network's users do not determine computational centralization – the relevant data point for a measure of computational centralization is whether nodes or miners are concentrated.

It is possible, where a governance token exists and there is reliance on token holders to vote on changes to a network, political centralization may be affected where there exists a high concentration of users in a certain jurisdiction or region. However, this hyper specific scenario did not justify use of the data point as a global measure of political centralization, and a measure of political centralization in that scenario would likely be adequately captured by other data points.

---

[87] *See, e.g.,* David Z. Morris, *Grin Founder "Ignotus Peverell" on Life After Launch, and the Path Forward (Feb. 27, 2019), https://breakermag.com/grin-founder-ignotus-peverell-on-life-after-launch-and-the-path-forward* ("By being anonymous, I'm also much less of a victim for people who'd want to influence me or profit indirectly from my position. I can be a good layer of insulation for contributors and developers directly involved in Grin: People can blame me instead of them. My anonymity avoids too much polarization, keeping the project more decentralized. I can't appear in public, do conferences and podcasts or tweet and that's a good thing.").

[88] *Id.* ("It means Grin has many public figures instead of just one").

GEOGRAPHIC DISTRIBUTION OF TRANSACTIONS

Transactions and network addresses may be controlled from within, and trade volume may occur within, a small geographical area. Although this may indicate some form of centralization exists – either computational or political – we believe the data points on Node Concentration and Node Communication adequately serve the purpose of taking geography into account.

GOVERNMENT AUTHORITY AND REGULATION

Governments may take a range of action regarding particular blockchains. In some cases, this metric will have been taken into account under Node Concentration, Concentration of Activity Among Code Contributors and Mining Power Concentration. In all cases, because government action tends to occur in a non-uniform manner, may involve anomalous fact patterns or fraudulent, non-existent blockchains, and often occurs after some determination that a network is centralized in some manner, or often in the absence of such a determination, the following data points do not weigh as heavily into the centralization analysis:

- The existence of laws that enable regulators or governments to seize or freeze native assets, or to formally investigate custodial entities such as exchanges with subpoena powers.
- Any attempts by a government to restrict or halt mining generally.
- The existence of a ban on trading of a particular asset, mining of that asset, on operating an exchange, or on selling a native asset.
- Whether any civil or criminal liability can attach to development activity. Note, however, that where such liability *can or does* attach to development activity, the collateral effect would be to encourage the industry to collaborate in order to share the costs of liability insurance.[89] A sea change in the form of a new developer liability regime might risk an increase of political centralization across the board. Such a change would require revisiting the political centralization analysis and its relevant metrics with the new developer liability regime as a backdrop.

GOVERNMENT CLASSIFICATION

In some jurisdictions, a blockchain's native asset may have been deemed to be a currency, security, commodity, or some other designation such as property. The formal classification of a native asset does not have any direct bearing on whether the network is centralized across any of the three metrics discussed above. The classification may correlate with the measure of political centralization (i.e., if deemed a security in the U.S., the more likely it is to be politically centralized), but any governmental designation would not make the blockchain network or native asset more or less politically centralized.

However, we note that where a government deems an asset to be a security, that classification can serve as a benchmark against which to calibrate one's measure of political centralization.

[89] *See also,* Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains* (July 19, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198.

HASH RATE

Hash rate, also known as hash power, is the measuring unit of the processing power miners are using to validate transactions on a blockchain. A consequence of a large hash rate is greater network security and increased resistance to a 51% attack, which may indicate a lack of network centralization. However, a large hash rate may also indicate an increase in miners joining the network, or increased mining difficulty generally, neither of which speak to network centralization. Furthermore, the hash rate itself does not reveal what percentage of the hash power is being controlled by individual miners or mining pools. A more reliable data point on this front, such as Mining Power Concentration, is listed above.

NUMBER OF FORKS

Where a blockchain network can be forked, anyone with access to the internet and sufficient knowledge can copy and paste the source code to launch another version of the network. Due to the potentially low barriers to forking, and the lack of any meaningful connection between the existence of a fork and either computational, economic, or political centralization, the number of forks is not a reliable indicator of network centralization. We acknowledge a contentious hard forks may affect some metrics meaningful to computational centralization, but any effect on computational centralization can be adequately measured by the metrics above on a pre-fork and post-fork basis, such as Mining Power Concentration.

NUMBER OF INDEPENDENT AUDITS

Developers will often hire independent security or code auditors to check their network's code for bugs or vulnerabilities. Politically centralized networks may call for ongoing independent audits from a community of auditors. These audits may result in a more secure network but would not make the network any more or less centralized by any measure. We therefore see no meaningful correlation between the number of independent audits and network centralization. While there may be a reliance on persons to arrange and pay for the audit, whether it be a foundation, DAO, or treasury fund, the Governance – Funds Deployment data point captures the relevant reliance concerns.

NUMBER OF TRADING PAIRS

Centralized exchanges may decide to list trading pairs for an asset for a variety of reasons. Decentralized exchanges may have no prerequisites to listing trading pairs. Thus, the number of available trading pairs is rather arbitrary, and cannot prove useful as a data point for measuring network centralization.

NUMBER OF TOTAL TRANSACTIONS

One sign of a mature network may be a high number of transactions since inception. One might attempt to argue that the higher the number of transactions, the more likely a network is not centralized. However, the high number may be a result of the existence of more validating nodes, the activity of trading bots, or simply that the blockchain has been operational for a long period of time. Thus the number of historical transactions is rather arbitrary and cannot prove useful as a data point for measuring network centralization.

SECOND LAYER PAYMENTS OR TRANSACTION MECHANISMS

Increasingly, blockchain developers create sidechains or other second layer mechanisms to address a range of issues with a network's inherent limitations. The existence of second layer mechanisms does not necessarily speak to whether a network is centralized or not. While they may only exist in networks that are generally considered to be decentralized, it is theoretically possible to build a second layer mechanisms on a completely centralized network.

SENTIMENT

Some analytics look to consumer sentiment as a predictor of market price, whereas the concept of economic centralization focuses on network addresses (the vertices) and the value they send (the edges) to other addresses. While consumer sentiment may indicate the likelihood of increased market activity, it does not directly inform whether a small number or a large number of network addresses will send value amongst each other. At best, it is an indirect measure of potential or economic centralization, and the direct measures listed above are more suited to the task of measuring activity between network addresses.

SOCIAL MEDIA

The impact of social media on a network will depend on whether it is run by an individual, organization or community volunteers, the amount of activity, whether the account is perceived or branded as official or verified,[90] whether the brand has been diluted by scams or other fake accounts,[91] amount of community interaction and their level of influence over the community. Social media may not necessarily impact Voting Control or Change Control (e.g., when used to spread awareness of a network or to provide updates), but has the potential to be used as a tool to assert influence with respect to Voting Control or Change Control (e.g., to coordinate airdrops, hard forks, code updates, inform the community of catastrophic bugs).

Where official accounts are controlled by a company, organization or foundation with IP controls over the network's branding, the use of social media to impact Voting Control or Change Control may indicate political centralization, as participants in a blockchain network may be reliant on the efforts of a small group of persons regarding the network's management or success. However, because social media is and has been used as a tool by key influencers, Existence of Key Influencers data point acts as a more direct measure of influence over network centralization.

TOP POOLS

A high concentration of mining power in the hands of a small number of mining or staking pools risks pool operator collusion and ultimately the ability to gain control over the hash power or voting

---

[90] *See About Verified Accounts,* Twitter, https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts#:~:text=The%20blue%20verified%20badge%20on,account%20name%20in%20search%20results (last accessed Aug. 8, 2020). *See also,* Jinia Shawdagor, *Crypto World Skeptical as @Bitcoin Twitter Account Ditches BCH Support* (Aug. 29, 2020), https://cointelegraph.com/news/crypto-world-skeptical-as-bitcoin-twitter-account-ditches-bch-support ("The @Bitcoin account has been involved in controversy in the past. Bitcoin supporters have criticized the account for its false advertising and misleading information that pushed people to believe that BCH is the true BTC.")

[91] See, e.g., Nikhilesh De, *Ripple Sues YouTube for Allowing 'Scams' That Promise Free XRP* (Apr. 21, 2020), https://www.coindesk.com/ripple-sues-youtube-for-allowing-scams-that-promise-free-xrp.

power on the network.[92] Such control would mean participants on the network may find themselves relying on the expertise of controlling pools to make crucial changes to the protocol. However, this data point is adequately captured by the Mining Power Concentration data point, and would be redundant if included.

TRANSACTION FEE

Transaction fees may vary over time, in part depending on network congestion. Transaction fees reflect network usage, but do not directly reflect network centralization. For instance, a popular application may temporarily cause increased network activity, congestion, and higher fees,[93] but the increased fee would speak more to the popularity of the application than the level of the network's centralization.

TRANSACTION SIZE

The size of transactions refers to the digital size of the data that corresponds to the blockchain entry. The more complex a transaction and the larger the amount of cryptocurrency being sent, the larger its data size. Transaction size may therefore reflect the complexity of a transaction, but transaction complexity is not necessarily related to network centralization.

UTILITY

Whether or not a native asset can be used, or has functional qualities, does not make the blockchain more or less likely to be centralized along any of the measures discussed. A native asset can be extremely useful, and its supporting network may still be politically, economically, or computationally centralized. Further, assuming utility is in fact meaningful to a measure of political centralization, measuring "utility" would not be possible without some further discussion regarding the term's definition.

*MISCELLANEOUS DATA POINTS

Finally, we determined without much controversial discussion that the following data points either (i) would not prove as useful to an analysis of network centralization as any of the data points listed above, or (ii) would not capture any additional concerns not already addressed:

- The existence of centrally owned media groups that may align with or advocate for use of a particular blockchain.
- The existence of a development incentive structure for wallet developers.
- The number of blockchain-specific conferences or events.
- The volume of independent academic work associated with a blockchain.
- The number of blockchain explorers available for a particular blockchain.
- The existence of blockchain-specific mining equipment or producers of such equipment.

---

[92] *See, e.g.,* Alyssa Hertig, *Bitcoin Cash Miners Undo Attacker's Transactions With '51% Attack'* (May 25, 2019), https://www.coindesk.com/bitcoin-cash-miners-undo-attackers-transactions-with-51-attack ("Two bitcoin cash (BCH) mining pools recently carried out what is known as a 51 percent attack on the blockchain in an apparent effort to reverse another miner's transactions.").

[93] *See, e.g., The Inside Story of the CryptoKitties Congestion Crisis,* Consensys (Feb. 20, 2018), https://consensys.net/blog/news/the-inside-story-of-the-cryptokitties-congestion-crisis/.

Conclusion

The list of data points above may change as technology and user habits evolve. We hope the proposed standards change along with the times, and that the industry gravitates more towards objective measures rooted in hard data when discussing concepts such as “centralization” or “decentralization.”

We recognize an active and robust dialogue among industry experts regarding how to quantify “decentralization,” and share additional resources here for those interested in further learning:

- Gabriel Shapiro, *Defining Decentralization for Law* (Apr. 15, 2020), https://medium.com/@lex_node/defining-decentralization-for-law-58ca54e18b2a.
- Lane Rettig, *The key ingredients to a better blockchain, Part II: Decentralization* (Sep. 15, 2019), https://www.etherean.org/blockchain/2019/09/15/key-ingredients-better-blockchain-part-ii-decentralization.html.
- Karim Helmy et al, *Measuring Bitcoin’s Decentralization* (Sep. 15, 2020), https://coinmetrics.io/measuring-bitcoins-decentralization/.
- Everett Muzzy and Mally Anderson, Measuring Blockchain Decentralization, https://consensys.net/research/measuring-blockchain-decentralization/ (last visited Oct. 21, 2020).
- Angela Walch, Deconstructing ‘Decentralization: Exploring the Core Claims of Crypto Systems (Feb. 13, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3326244.

If you would like to discuss any portion of Ketsal’s proposed standards, please reach out to the authors at josh@ketsal.com or jenny@ketsal.com.

Appendix: Data Points as Applied to the Bitcoin Network[94]

Data Point	Value	Notes	C	E	P
Block Size	1 megabyte (yearly average: 1 MB) (historical high: 1 MB)	Block size, with additional comparative metrics in parentheses.	•		•
Circulation *Distributed*	18,393,043	Number of the native asset already distributed and available to transfer.		•	
Circulation *Not Yet Distributed*	2,606,957	Number of the native asset not yet distributed (assumes a cap of 21,000,000).		•	
Client Software *Availability*	13 (Bitcoin Core, Bitcore, Bitcoin Knots, BTCD, Bitcoin UASF, bcoin, TRB, Bitcoin Unlimited, Bitcoin XT, btc1, Bitcoin Classic, libbitcoin)	Client software available (data source: https://coin.dance/nodes).			•
Client Software *Popularity*	Bitcoin Core (97.8%)[95]	Name of the most popular client software and percentage of nodes using the software (data source: https://coin.dance/nodes)	•		
Compensation	Null	Percentage of fees and premined assets designated to developers.		•	•
Concentration of Activity Among Code Contributors	21.65%	Percentage of commits from the top 5 contributors.			•
Cost of Running a Node	~$9.6/day	Estimated daily cost of running a node for 1 year. **Note**: Cost varies widely; the estimate is NTerminal's proprietary measure.	•		
Exchange Listings	155	Number of exchanges reporting active bitcoin trades within NTerminal.		•	

[94] Some data points provided by Inca Digital via NTerminal. All data points are current as of June 3, 2020, unless noted otherwise.

[95] As of Sep. 18, 2020.

Existence of Key Influencers	Yes, 5	Count of persons including the lead maintainer and maintainers.		•	•
GitHub Project Statistics	25854	Number of GitHub forks of main repository.			•
	7.85	Average Contributor account age (in years) on main repository.			•
	43619	Number of GitHub stars on main repository.			•
	3498	Number of GitHub subscribers on main repository.			•
	894	Number of GitHub open issues on main repository.			•
	389	Number of GitHub open pull requests on main repository.			•
Governance *Development Efforts, Network Control, and Updates*	Off-chain voting	On-chain or off-chain voting?			•
	Null	Voting restricted to issues put forth by maintainers?			•
	Null	Existence of board or foundation to exercise significant influence over protocol changes?			•
	Yes	Protocol software changes subject to community (or miner) vote?			•
	Null	Existence of kill switch, backdoor, control over an oracle, listing permission, or ability to remove a project?			•
	Yes	All proposals can be put up for voting?			•
Governance *Funds Deployment*	Null	No mechanism to deploy funds beyond block rewards to miners.			•
Intellectual Property	Null	To our knowledge, no IP rights would prevent use of “bitcoin” with respect to			•

		payments protocols or prevent further forks.			•
Issuer Influence Over Exchange Listings	Null	No issuer influence over cryptocurrency exchanges wishing to list those assets.			•
Liquidity Provision	Null	No issuer provisions to provide liquidity.		•	•
Market Attack Cost	**Note:** This metric is theoretical for the time being.	**In theory:** The least amount of financial resources it would take to cause a Market Crash e.g. by selling a significant amount of native assets or taking a short position.		•	
Mining Power Concentration	58.64% (f2pool, poolin, btc.com, antpool)	Percentage of blocks mined by the top four mining pools over the last year.	•	•	•
Network Attack Cost	$4,463,906.57 (per hour)[96]	NTerminal 51% attack cost metric.	•		•
Network Completion	Complete	Status of network.			•
Node Communication	1861ms (transactions), 399ms (blocks)	Average speed for propagation for 50% of the inv messages to reach first 1,000 nodes over the last year (data source: https://bitnodes.io/).	•		
Node Concentration	56.66%	Percentage of detected nodes clustered to the top 4 countries. **Note**: This metric is highly unreliable currently.	•		•
Number of Contributors	362	Number of GitHub contributors on main repository.			•
Number of Maintainers	5	Michael Ford, Wladimir van Der Laan, Jonas Schnelli, Marco Falke, Samuel Dobson			•
Number of Nodes *Full Nodes*	10,465 reachable nodes[97]	Number of full nodes (data source: https://bitnodes.io).	•		

[96] As of August 20, 2020.

[97] As of August 26, 2020.

Number of Nodes *Validators*	*[no reliable data available at publication time]*	Number of validators (i.e., number of miners).	•		
Permissive License	Yes	Available on GitHub for public comment.	•		•
Potential to Access Material Non-Public Information	Low	The code is open source and is broadly utilized. However, bitcoin bugs can be reported anonymously to security@bitcoincore.org, which cannot be publicly accessed.			•
Release Mechanism	Proof of work	Mechanism of native asset distribution.		•	•
Stake *Postmine Distribution*	null	No postmine.		•	•
Stake *Premine Distribution*	null	No premine.		•	•
Stake *Percent Held by Largest Holders*	14.78%	Percentage of circulating supply held by top 100 addresses.		•	•
Stake *Percent Held in Exchange Wallets*	13.00% (2.400,517 in exchange reserves / 18,469,000 circulating supply)[98]	Percentage of circulating supply held in exchange wallets (data sources: https://cryptoquant.com/overview/btc-exchange-flows & https://www.blockchain.com/charts/total-bitcoins).		•	•

[98] As of August 23, 2020.