UNIVERSITY OF EDINBURGH
Business School

A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors

by

Nic Carter

Dissertation presented for the Degree of MSc Finance and Investment

2016/2017

Abstract

Cryptocurrencies and their conceptual cousins – tokenized networks – represent a growing and still largely unregulated asset class. These draw upon the principles of free open source development and inherit governance structures from them, while introducing protocol-level economic incentives. This paper describes and analyzes governance models in these projects. This empirical study of fifty tokenized networks finds that governance structures are largely informal, obscure to investors, and characterized by the concentration of decision-making and funding. Innovations such as Proof of Stake, masternodes, and protocol-level tokenholder governance grant investors some governance rights, yet reliable implementations have not yet emerged. While decentralization is a stated goal of many of these projects, political governance in practice is highly centralized. This represents an overlooked risk factor for investors in this novel asset class.

Glossary

ASIC: Application Specific Integrated Circuit; used to efficiently mine cryptocurrency; optimized for specific algorithms.

Bitcoin: a decentralized protocol for the transfer of peer-to-peer digital cash.

bitcoin: the token that circulates on the Bitcoin protocol; the native unit of exchange.

Block reward: periodic payments to cryptocurrency miners who solve computational puzzles, or stakers who are allotted new tokens and fees.

Blockchain: a shared ledger upon which new entries – organized into blocks – are continually inscribed.

CoinMarketCap: a popular website for comparing cryptoasset price and network value.

Copyleft: open-source software licensing model whereby derivative products have to follow the same licensing.

dApp: Short for distributed application; applications which run on a distributed basis, commonly hosted on the Ethereum protocol.

Darknet: the un-indexed internet; hosts websites used to exchange cryptocurrencies and illicit goods.

Distributed ledger technology: the technology that the Bitcoin protocol is based upon.

Ethereum: a decentralized computing platform aimed at running distributed applications and smart contracts; the native token required to incentive the network to conduct computational tasks is ether.

Fiat: fiat currency issued by governments, such as the US dollar.

FOSS: Free Open Source Software. It is both free to use and transparently developed.

Github: a popular code repository where developers share and contribute code.

Hard fork: an incompatible change to a software system.

Masternode: a node which carries out tasks on a cryptocurrency network in exchange for a share of block rewards and voting rights.

Miner: a network node which carries out computational tasks in exchange for block rewards. Also used to refer to individuals who run such nodes.

Network value: this figure is determined by multiplying the cryptoasset units in circulation by their trading price. A common means of cryptoasset comparison.

Premine: a tactic by developers launching Proof of Work cryptocurrencies to mine some quantity of the cryptocurrency for private benefit prior to public release.

Proof of Stake: a consensus algorithm in which network influence is determined by the share of tokens held; these must be staked to earn block rewards. Staked systems can allocate voting power to stakeholders. Abbreviated to PoS.

Proof of Work: a consensus algorithm in which miners compete to earn a fixed issuance of periodic block rewards. Influence is measured by hashpower. Abbreviated to PoW.

Protocol: a set of rules defining interactions between entities in a system.

SegWit: short for Segregated Witness, this update was developed for Bitcoin to solve a variety of technical problems and to lay the groundwork for Bitcoin as a settlement system with a payment layer on top. It was activated on Bitcoin in August 2017.

Slack: a messaging platform, popular with cryptoasset developers and investors.

Slock.it: a startup which wrote the initial code for The DAO and planned to administer it.

Soft fork: a change to a software system which is compatible with previous versions.

The DAO: short for the decentralized autonomous organization, this was a venture capital organization where funds were pooled and governance was shared among tokenholders; this was launched on the Ethereum platform in 2015 and was dissolved after the contract code was exploited by a hacker.

Token: a unit circulating on a cryptoasset network; these may have intrinsic use, be redeemable for goods or services, exist to incentivize the adoption and use of a network, exist for fundraising purposes, grant voting rights, or have no rights or use whatsoever.

Tokenholder: conceptually equivalent to a shareholder, a tokenholder is someone who owns cryptoasset tokens. Token ownership grants in some cases claims over network governance and capital return, although these are not legally enforced.

UASF: short for User Activated Soft Fork, this was a popular movement by some in the Bitcoin community to overrule miner resistance to the SegWit upgrade and force it through by threatening to deny certain miner traffic access to network nodes.

Table of Contents

I. Introduction

In 2008, the notion of a cryptocurrency entered the public consciousness through an obscure cryptographic mailing list. The pseudonymous Satoshi Nakamoto released a paper and a software client solving, for the first time, the double-spend problem of digital cash. Since then, distributed networks based on this technology have grown into a 100-billion-dollar industry. The Bitcoin protocol was supplemented by numerous clones offering slight variations on the original, and eventually redesigned networks which aimed at fulfilling other use cases. Early innovations included domain registry, anonymous transactions, faster transactions, time-stamping, and smart contracts.

Permissionless distributed ledgers, originally designed to decentralize the control and issuance of monetary units, were repurposed for a myriad of other uses. As the value of these networks grew, developers devised a variety of methods for giving investors exposure to these projects. Alternatives to the Proof of Work consensus function were developed, including the popular Proof of Stake consensus mechanism, which does not require costly computational resources. In recent years, the Initial Coin Offering (ICO), or token offering, has become a popular method of issuing tokens connected to distributed networks. These involved the presale of tokens tied to the value of an underlying network, application, or protocol. These token sales caught the attention of the U.S. Securities and Exchange Commission (SEC), which issued a cautionary note about the sale of unregistered securities in July 2017. Additionally, with the aid of smart contracts, new structures emerged, including distributed anonymous organizations (DAOs) or distributed anonymous corporations. These promised to redefine the very nature of the firm; DAOs were designed to be jurisdictionally untethered, collaborative organizations controlled only by the democratic consensus of participants. Thus drawing on the principles and the design of the original cryptocurrency, an incredible variety of networks emerged.

Investor protections in this novel industry are limited, for several reasons: regulators have not had sufficient time to grasp the nature of this new technology; developers and promoters can distribute tokens to investors from virtually any jurisdiction, complicating enforcement; regulators are muddled on whether digital currencies and distributed tokens represent a new asset class or a rebrand of an existing one; anonymous developers, investors, and exchanges with poor KYC/AML complicate the tracking of these assets; and there is a colossal amount of variation in the nature and design of these distributed networks.

This paper is an attempt to codify and differentiate these heterogeneous projects with regards to their organizational structures. This empirical survey looks at a snapshot of the fifty most valuable networks (together representing 99.3% of outstanding network value when the snapshot was taken) in order to define how these networks are governed. Since little work has been done in this space, much of this work is descriptive rather than analytical; however, even this limited approach holds use for investors, regulators, and developers. Inevitably, the qualitative judgments made in this study leave some room for disagreement. This is the nature of an investigation into projects that have no disclosure requirements.

To date, this is the most comprehensive survey of power structures in these distributed networks. While particular attention is given to political structure, this study also captures developer funding methods and transparency. This study has dual motivations: it makes the case for the existence of governance mechanisms on every network, even if they are implicit, and reveals the industry's inability to generate meaningful investor governance despite common appeals to decentralization.

Decentralization is held in cryptoasset communities as a valuable quality. It is treated here as a multi-dimensional concept, requiring dispersion not only at the node and protocol levels, but also at the governance level. A diverse set of governance models are employed, but the majority concentrate decision-making and fiscal power in the hands of a corporation, foundation, or small group of individuals. This exposes them to regulatory risk, and raises the risk of expropriation.

This paper is structured as follows: first, the qualities of cryptoasset networks as investable assets are considered, and some asset class features are described. Then cryptoassets are sorted into conceptual bins for better in-group comparisons. The value proposition of these networks is considered, and the multi-dimensionality of decentralization is introduced. Evidence from a survey of the largest projects is then presented. Contrasting governance models are detailed and incentive structures explained. Conclusions for investors, regulators, and entrepreneurs are drawn.

Literature review

Since cryptocurrencies have only existed since 2008, and Bitcoin was virtually the only one in existence until 2012, literature is sparse. Additionally, since Bitcoin superficially appears governed by an emergent consensus between miners, developers, and users, little attention was paid to its governance until it reached an impasse over scaling. Previously, miners (owners of computers performing network tasks) had just rubber-stamped the technological decisions of the core developer team. Nonetheless, some literature exists to provide context for this novel topic.

The Bitcoin whitepaper by pseudonymous creator Satoshi Nakamoto (2008) describes the technical design of the system and the finely-poised incentive structure. An introduction to bitcoin and cryptoassets as a novel asset class can be found in Burniske and White (2016), as well as in Elendner et al (2016). Burniske and White influentially make the case for bitcoin as a novel asset class, on investability, politico-economic, correlation, and risk-reward grounds. Notably, they find a complete lack of meaningful correlation between bitcoin and any index, commodity, or currency, which continues to be the case today (Blanch 2017). Bitcoin's investability has increased dramatically since their paper, with deeper liquidity and the announcement of a Bitcoin derivatives desk regulated by the Commodity Futures Trading Commission.

Cryptoasset governance is poorly catalogued, although these assets belong to the superclass of entities known as free open source software (FOSS) projects, which have been studied at length. Traditional corporate governance considerations do not apply directly to cryptoassets, as they have historically been open-source, volunteer-based, and unincorporated, and hence rejected traditional corporate structures. Investors and speculators in cryptoassets like bitcoin are granted no shareholder rights or protections. Decision-making in bitcoin and most cryptoassets is a function of developer teams releasing software which is algorithmically ratified by miners and stakeholders. Cryptoasset projects crucially differ from traditional open source networks in that ownership is demonstrated through the possession of tokens and hashpower, which can be used to signal intent. Together with the explicit ascription of value to these networks, another departure from typical open source projects, a variety of experimental governance models have sprung up in this space. These are motivated by a demand on the part of tokenholders to obtain shareholder governance rights over their investments, or to incorporate formal structures for efficiency gains.

A general introduction to the implications of blockchain technology on governance processes comes from Yermack (2017). Although he does not mention how popular blockchains are administered, he notes that blockchain technology can facilitate transparent, irrevocable votes, real-time accounting, and public ownership. These are all mechanisms that are employed in some of the governance models discussed here. Interestingly, he notes that activist investing may be complicated by transparent ledgers, as this reduces flexibility and stealth in position accrual.

The multi-tiered cryptoasset governance model that this paper relies on is introduced in De Philippi and Loveluck (2016). They argue that bitcoin exhibits governance on the protocol level (through the formal algorithmic functioning of the Bitcoin protocol) and on a subtler basis with regards to decision-making about the software itself. De Philippi and Loveluck argue that this latter governance is highly technocratic and invisible to most observers, and indeed, highly centralized. They challenge the notion that Bitcoin is inherently trustless, arguing that the core developers are granted a significant level of control over the development of the protocol. In particular, they note that while anyone is free to submit an improvement to the network, the final call lies exclusively with the core development team. Through the analysis of the political nature of a technical debate over scaling, De Philippi and Loveluck argue that governance is heavily concentrated and oligarchic, suggesting instead a more open and transparent institutional structure. Recent developments have however challenged the notion that core developers wield ultimate power in the system however, with miners, industry groups, and community-organized revolts all playing significant roles in the continued debate over scaling.[1] Nonetheless, De Philippi and Loveluck introduce the multi-layer governance structure that I will draw upon here.

Reijers, O'Brolcháin, and Haynes (2016) compare the Ethereum and Bitcoin governance models through the lens of social contract theory, concluding that no functioning formal models of blockchain governance exist. Their principal contribution is to frame the organization of blockchain communities as overtly political entities, even though their founders commonly seek to position them as purely technical communities. Finally, Yarvin (2016) provides a useful post-mortem on The DAO, an innovative tokenized network that attempted to delegate power to token-holders.

[1] A detailed discussion of Bitcoin's governance is outside the scope of this paper; for more on this, see Appendix C

Literature on decentralized governance more generally is instructive. This stretches beyond the financial corporate governance literature towards political science and sociology. In their survey of twelve multistakeholder governance models, Gasser, Budish and West (2015) find factors which are critical to success. These are inclusiveness (within reasonable constraints), transparency, accountability, legitimacy (context dependent), and perceived efficiency. They find no best way to govern groups of diverse stakeholders, and note hierarchical and consensus-driven groups both finding success. The most successful projects were able to adapt to changing contextual conditions.

Coglianese is less optimistic; in his 1997 study of consensus-building among regulators and other stakeholders, he finds that required consensus thresholds (such as those found in Bitcoin and many Proof of Work systems) lead to least-common denominator outcomes, stalemates, and cannot be rushed. All of these tendencies are exhibited in Bitcoin, which has extremely high consensus thresholds for software activation. Ansell and Gash, in their widely-cited 2008 study of collaborative governance, find that initial leadership is crucial to establish ground rules and build trust; and that the most important features of a collaborative institution include clear rules of engagement, transparency and inclusiveness, and a single forum of engagement.

Several authors specifically cover the governance of open-source networks. These are generally non-corporate, but may be foundation-guided. Power structures are diffuse and often poorly defined. Foundational in this space is Raymond's (1997) analysis of governance modes in open source, based on the Linux project. He specifies two contrasting models of distributed governance in collaborative software projects, defining them as anarchic (bazaar) or hierarchical (cathedral). De Laat (2007) builds on this in a cross-sectional study of multiple FOSS projects; he does not offer guidance on optimal open-source governance configurations, adding that a variety of models have demonstrated success. Jensen and Scacchi (2010), in a longitudinal analysis of the popular open-source project Netbeans, find that developers self-organize into hierarchical networks. Neither the bazaar nor the cathedral model suit their findings. They find that Netbeans exhibits formal protocol and informal extra-protocol governance; routine procedures are codified, and more complex decisions and revisions of the procedures themselves are driven by a more informal, social norms-based process. Controversies resulted when decisions were made untransparently, or without buy-in from the community. They add that ungoverned open-source projects tend to fall into chaos, as some decision-making norms

are required. Finally, Franck and Jungwirth (2003) describe the intentions of developers in open-source networks, describing them as voluntaristic or rent-seeking, and explaining how both can coexist in a single network.

This study also draws on Van Valkenburgh (2016) and Brito and Castillo (2016) for a discussion of securities laws as they relate to cryptoassets, and Bentov et al (2014) for a discussion of the Proof of Stake algorithm, which introduces the mechanism which allows tokenholders some governance rights.

Cryptographic protocols and tokenized networks

The Bitcoin protocol, first published in 2008, proposed a solution to the “Byzantine generals” problem: this refers to the difficulty of establishing trusted communication with a partner in a network (Lamport, Shostak, and Pease, 1982). Bitcoin accomplishes this by establishing rules which promote a single shared ledger (“blockchain”) which hosts a common history of the network. Through public-private key cryptography, nodes can trivially verify that a transaction is valid, and that users have the funds they claim to have (Nakamoto, 2008). This prevents the double spending of funds, a common problem in digital cash networks.

Bitcoin secures an honest history of the network by aligning incentives: nodes that perform computational tasks (“miners”) are rewarded with newly issued tokens in exchange for supporting the blockchain. Since these tokens only have economic value if the system is protected from attacks and functions as expected, miners are incentivized to promote an honest history of the network. Thus validation is performed instead by a disparate group of miners who support the network with computation power.

Since the computation work requires resources (electricity and computer hardware), miners only support the Bitcoin protocol if the tokens periodically disbursed by the network have economic value (or the miners mine them speculatively). The expensive network security, ensured by the Proof of Work algorithm, requires the circulation of incentives, represented by the units of value, known as bitcoin. Hence the protocol is inseparable from the economic incentives that underscore it.

Therefore the protocol provides a way for heterogeneous parties to mutually agree on the ownership and transfer of digital property, where no cooperation is assumed, and no third

parties are required. This is a genuinely novel technological innovation. Bitcoin mediates the transfer of value, although similar protocols could be adapted to enable the transfer of any digital good.

The periodic issuance of tokens to miners also solves the problem of how to distribute a novel currency. However, since economies of scale exist, miner activity tends inevitable towards concentration. Today, Bitcoin is mined chiefly by a few large industrial participants, many of whom are located in China.[2] Since miners have significant control over network upgrades, concentration of power among miners is considered a threat to the network. Thus an alternative method of verification for cryptocurrency networks emerged. This innovation was known as Proof of Stake ("PoS"), first formalized by King and Nadal in 2012. In a staked digital currency, network rewards are distributed relative not to individual hashpower, as with Proof of Work, but relative to the ownership of tokens in the network. Larger stakeholders have a proportionally better chance of generating the next block and collecting transaction fees, or newly minted tokens, if they exist. Under Proof of Stake, no energy is directly consumed to generate network security, as with Proof of Work (although Paul Sztorc has argued that work is nonetheless consumed and PoS is merely "obscured PoW" (2015a)).

However the problem of how to initially distribute the tokens persists. Since network security depends on faithful stakers, not the periodic issuance of tokens, PoS systems can be initiated with a complete set of tokens in existence. This raises the importance of the initial distribution model, which is heightened by the fact that stakers gradually accumulate network rewards proportional to their ownership. If participants do not stake, their share is diluted and network benefits accrue to those who do. Thus it is possible for large block-holders in PoS systems to accumulate and retain significant power due to poorly publicized or obscure initial distributions, and through the redistributive properties of PoS. In a PoW system, transaction fees and block rewards accrue to miners, but the continuous costs of a computationally demanding operation require periodic sales of tokens by miners. This ensures a churn and a wider token dispersion, relative to a PoS system in which large tokenholders have no immediate pressure to circulate their tokens.

[2] Distribution of Bitcoin hashrate and the identities of miners can be found on a web tracker such as Blockchain.info

Proof of Stake systems also create opportunities for voting, in those cases allocating power on a proportional basis to the share of tokens held. This grants tokenholders some formal power over the governance of a network, which in Proof of Work systems is generally distributed informally among developers, network nodes, and miners. While emergent governance structures exist in PoW, formal tokenvotes in PoS usefully codify power relationships. That said, tokenvotes are beset by concerns over concentrated token distributions, poor transparency, and voter apathy.

Since 2008, following Bitcoin's early success, a huge number of imitators and innovators have come into existence. Many of them are only slight modifications of the original platform, but some novel cryptographic and tokenized networks have also arisen. While Bitcoin retains its lead as a peer-to-peer value transfer network, other qualitatively different networks have launched. These cover use-cases as diverse as distributed data verification, smart contracts, data storage, private transactions, and prediction markets. Common features include distributed networking, and the securing of economic incentives with tokens, but significant disparities exist, which bear noting. Mainstream commentators often refer to the entire asset class as "cryptocurrencies" even though only a selection have currency-like features.

II. Exploring and codifying the new asset class

As Van Valkenburgh says, "[cryptocurrencies] present an arrangement of technological components that is so novel as to defy categorization as any traditional asset, commodity, security, or currency" (2016).

In Bitcoin's case, various US governmental bodies has defined and regulated it as a commodity (CFTC, 2015), as a virtual currency (FinCEN, 2013), and as property (IRS, 2014). This considerable regulatory confusion as to the classification of cryptoassets is a function of their fast-changing and heterogeneous nature. This paper seeks to split these networks into categories that reflect their purpose, function, and use.

Dis-aggregating cryptoassets

The Bitcoin protocol was labeled a "peer-to-peer electronic cash system" and an "electronic payment system" by its creator in 2008 (Nakamoto). It came to be known as a cryptocurrency. Due to the rigors of launching an entire monetary system, it includes provisions for transactions,

circulation, minting, and security. Hence the Bitcoin protocol is a novel monetary system, on which the bitcoin currency circulates. Features of the Bitcoin protocol have been adopted for use in other open source cryptographic protocols. These have commonly been called cryptocurrencies as well. For instance, Vitalik Buterin, the creator of the smart contract platform Ethereum, referred to it as a cryptocurrency in its initial white paper in 2014. But ether, the token circulating on Ethereum, bears a different categorical treatment, since its properties and use case differ significantly from those of bitcoin. Bitcoin seeks to circulate and store value electronically; ether is a token used to purchase computing space on the Ethereum platform to run distributed applications (dApps). While ether can be used as a means to transmit value, its intended use is to "incentivize computation within the network" (Wood 2014).

Some tokens, like ether, have an intrinsic use within their protocol, others are created to raise capital for developers and to grant subsequent access to future networks, and others are straightforward digital currencies competing with fiat. These distinctions are not trivial; they hold implications for developers, investors, and regulators, some of which are discussed here.

Therefore to eliminate ambiguity and efficiently communicate the differences between these digital goods, I propose the following taxonomy, visualized in *Figure 1*. Broadly, tradeable tokens circulating on distributed ledgers can be referred to as cryptoassets. Major distinctions relate to the token's value on the platform or protocol itself. A distinction is also made between cryptocurrencies and platform tokens.

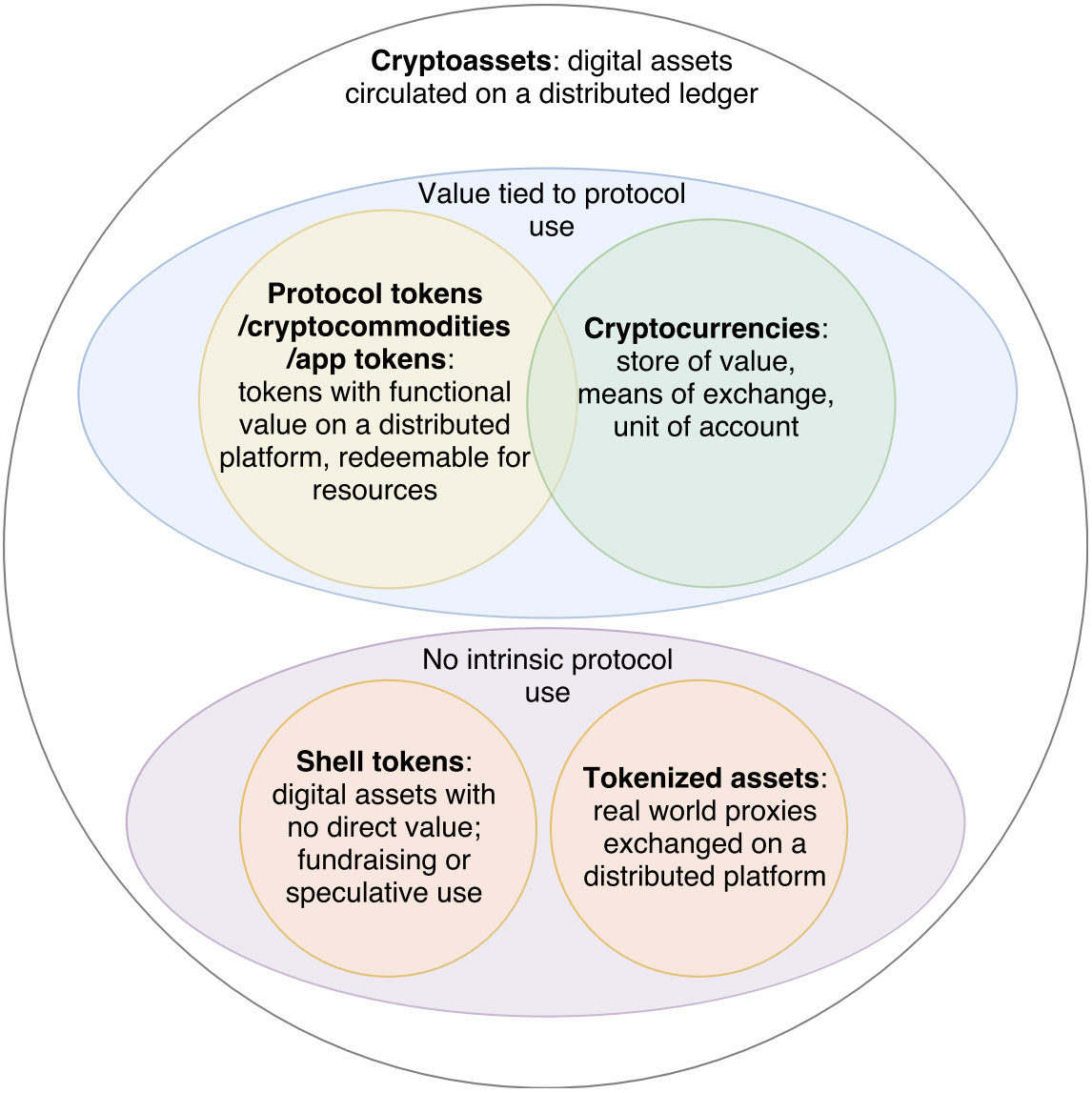


Figure 1, a cryptoasset taxonomy

First, a note on “cryptocurrencies.” This usage contrasts with “digital currencies” or “virtual currencies” which are the terms commonly employed by regulators. Since the vast majority of US dollars are held and transmitted electronically, it could be argued that the dollar is a digital currency, and the distinction falls apart. And while some cryptoassets are designed explicitly as currencies, their nature more closely aligns them with property or a scarce asset like gold.

For instance, bitcoins themselves do not circulate, but rather their ownership does. There are a finite number in circulation (when the last bitcoin is mined, there will only ever be 21 million) and

so their exchange rate is a function of scarcity rather than any central bank. No agent exists to mollify boom-bust cycles, and indeed bitcoin is characterized by them (Garcia et al, 2014). Their unit value is arbitrary, as they are divisible to eight decimal places, and developers could trivially increase this number. Bitcoins are programmable. Additionally, distributed currencies like bitcoin differ from centrally-issued digital currencies such as those used in games like World of Warcraft, and this distinction should be upheld.

Therefore "cryptocurrency" is already a more apt monitor than virtual currency or digital currency. However, as mentioned, the majority of assets in this loose category are neither designed nor function as currencies. These deserve further segmentation.

The first major attempt at developing a consistent taxonomy comes from Burniske and Tatar (2017)[3]. They provision cryptoassets into cryptocurrencies, cryptocommodities, and cryptotokens. Cryptocommodities in their analysis are the value units of blockchain networks that provision basic digital goods, such as "compute power, storage capacity, and network bandwidth." These can be easily compared to physical commodities like gasoline, corn, or cobalt. While the value of cryptocommodities is more difficult to ascertain, it is directly tied to that of the protocol, as the protocol demands payment in its constituent token. The most visible cryptocommodity is ether, which is required to power computations on the distributed Ethereum network.

Burniske and Tatar also segment the market into cryptotokens, which are the tokens connected to "finished product" digital networks. These tokenized finished goods include tokens like STEEM (token incentivizing participation on a social media network) and REP (token rewarding users who power the decentralized prediction market). The division between cryptocommodities and cryptotokens is obscure, however. Tokens like ether (computing power), SJCX (storage), MAID (storage), GNT (graphical rendering) have similar incentive structures to their finished good counterparts: buy a token to participate in a decentralized network. While the services provisioned by tokens seem more fundamental than others, the basic structure is the same. The division seems not between different quality goods, but rather the potential for direct usage on a platform or protocol.

[3] Publication forthcoming; extracts published with special consent of the author.

Thus I don't differentiate on commodities versus finished goods, but rather tokens with intrinsic protocol usage versus shell tokens. Shell tokens are projects where tokens are issued speculatively, with little backing, vaporware, or an unfinished protocol. Previous token taxonomies have omitted the existence of shell tokens, which deserve a mention, as they represent a significant risk factor for investors. To many investors, they are indistinguishable from protocol tokens, and founders are incentivized to obscure this difference. Currently, the majority of the hundreds of assets listed on popular websites like CoinMarketCap are shell tokens, with poor, absent, or closed-source development, no community backing, and no viable product. These are frequently run by anonymous or untransparent developer teams, with corporate structures in tax havens, and the distribution of tokens is often obscure. Power is often concentrated in a few individuals. Determining whether a token performs its stated purpose, or is simply an extractive shell token is often difficult, due to the lack of disclosure requirements and the low levels of professionalization in the industry. However, key factors that alert investors to shell tokens are the lack of a community supporting the project, the existence of corporate entities that control decision-making and funding, large or unclear token reserves held back for founders, closed-source or lacking development, and general poor transparency.

A final distinction that I make separates app tokens and platforms (although this division is more granular and not included in the diagram). Ethereum is a platform or protocol upon which other assets can be built. Platforms are poorly interoperable and generally mutually exclusive with each other. Demand for platform tokens derives in large part to their use in securing assets created on their platform, as is the case with Ethereum. Since the industry is still in its infrastructure-building phase, platforms are the most popular entities in the top 50 list. However, some assets have smaller ambitions – to capture a single use-case and dominate it. These are called appcoins or app tokens. While the difference between platform tokens and app tokens is abstract, app tokens can be recognized based on the clear connection between the service they provide and the token's value. Hence for an app token like Siacoin, the token itself represents the right to obtain data storage from the distributed application. While the nomenclature employed here is not authoritative, clearly defining divisions within the asset class enables investors to think clearly about the assets and alerts them to key risk factors.

The free and open-source network structure

Free and open-source software (FOSS) refers to software which is free to use and modify, without any entity controlling intellectual property rights. This became popular in the early 90s

when the Linux operating system was developed and released. Generally, FOSS projects operate under a licensing system in which attribution is preserved, and under a copyleft stipulation, whereby subsequent versions of the software maintain the same licensing rights. As Marshall (2006) notes, this licensing structure has a viral effect, whereby subsequent versions of the software remain open. As de Laat notes, FOSS networks are frequently born out of a desire to rebel against an incumbent; Linux, for instance, was motivated in part by Microsoft's monopolistic control over operating systems at the time (2007). De Laat's empirical study finds that the pareto principle applies in FOSS development: a small minority of programmers are responsible for a majority of the code. While many are structured as meritocracies, the non-uniform distribution of programming talent means that inevitable hierarchies result.

Investigations into open-source governance yield a staggering diversity of approaches. While decision-making is necessarily concentrated, these differ between benevolent dictators (in the case of Linux) to semi-decentralized systems like Apache, Debian, Gnome, Mozilla, and Netbeans (De Laat 2007). Some maintain barriers to entry for developers: Debian required a formal, sponsored application, and FreeBSD and Mozilla both had putative developers take exams. A wide variety of explicit governance structures are evident among successful FOSS projects: this stretches from autocracy (Linux) to closed committee votes (Perl, Mozilla), to democratic processes (elected leaders in Debian and FreeBSD, developers electing the board in Netbeans). Additionally, De Laat notes that all major open-source projects ultimately created foundations to facilitate intellectual property ownership and donor transactions. These foundations were often set up to remain distinct from the FOSS projects, but in some cases came to wield significant power over them. He adds that enterprise capture of FOSS projects through foundations is a legitimate threat to their independence.

De Laat's analysis suggests that a variety of governance structures can underlie a thriving FOSS network, although some degree of decision-making centralization is inevitable. This analysis extends only to the meritocratic, largely un-politicized FOSS communities that existed prior to Bitcoin's creation. The crucial difference between cryptoassets and other open-source software networks is the direct insertion of economic value into the protocols themselves. This complicates leadership, raises incentives to attack the system, and dramatically raises the stakes of the governance structure.

Why do individuals contribute their free time to open-source projects that they do not directly profit from? The literature provides two competing theories: the rent seeker and the donator hypothesis. The former, proposed by Lerner and Tirole (2002), suggests that individuals profit from their labor in FOSS networks through placements on a secondary labor market (in consulting or venture capital). The expertise gained and crucially signaled to market players is worth the initial investment of costly labor. The donator thesis suggests that individuals are ideologically motivated to work to create a public good – for Linux, an open source operating system; with Bitcoin, an open source means of transmitting value. Franck and Jungwith (2003) blend the two nimbly, suggesting that FOSS network structure can reconcile the two development approaches. They suggest that the copyleft licensing structure accommodates both the donators (by satisfying their desire to create a lasting public good, and protecting against the monetization of their software) and the rent seekers (by allowing them to monetize reputation gains on the secondary markets).

Cryptoassets draw on the traditions of open source, while maintaining some crucial differences. Many projects share the rebellious traits of open source software projects against corporate incumbents, and attempt to establish a public good. One such public good would be censorship-resistant, globally usable sound money. The language of open source, voluntaristic development, and free usage is common. Centralized, inefficient intermediaries are commonly targeted, rather than exploitative closed-sourced software.

Crucially, however, value is embedded into these tokenized platforms. This represents a key departure from the FOSS network tradition, as these could not easily be monetized and developers had difficulty financing their efforts. The ability of development teams to hold some portion of the tokens in reserve, or withhold a piece of every block mined, directly aligns the success of the tokenized network with their own financial gain. Although not every set of developers pay themselves like this, and many still work for free under the prior protocol. Interestingly, corporate entities have recaptured the space, using the language of communitarian, open source public good promotion, while simultaneously developing conventional closed-sourced, non community-backed software. The rebellious ethos which incentivized developers to work for free has been coopted to some degree by corporate entities. Finally, rent-seeking becomes much more direct and immediate, and developers no longer need to rely on secondary markets to monetize their involvement, although this still does occur. Donators can still contribute to public goods, although incentives to expropriate are elevated.

Features of the new asset class

1. Airdrops and hostile spinoffs

One method of token distribution which is perceived to be equitable involves an airdrop – this involves granting tokens to every address on a protocol (for instance, bitcoin) on a given date. This was the method of distribution employed by Clams, Byteball, and Stellar. These then could be traded on the open market and bitcoin owners not wishing to use those networks could collect a “dividend”. Neither Clams, Byteball, nor Stellar was perceived as a direct competitor to Bitcoin, so the airdrop was politically neutral.

These airdrops are similar in nature to a “fork,” although forks generally compete for the same network. A fork is simply an edit of the code which then competes for attention with the parent code. It can be launched with universal consent, or only a small fragment of users of the parent network. Forks can range from simple implementations of new code, to experimental side-projects, to contested battles for supremacy over the soul of a network. The issue with an ungoverned open source project is that it faces constant Ship of Theseus difficulties – absent a benevolent dictator, no one is empowered to declare what values are sacred to the protocol. Thus in the case of a contested hard fork, incompatible with the previous network, there is no single arbiter of which one constitutes the “real” chain. Until summer 2017, Bitcoin had never suffered a contentious hard fork, although it has hard forked (with the assent of miners) to fix a technical glitch in the past. Ethereum, despite centralized leadership under a benevolent dictator, suffered a contentious hard fork in July 2016, and the community split irrevocably, although the leader’s chosen chain predominates today.

Whether a hard fork is a threat to the network or not is a question of whether it has universal assent within the community. As Bonneau et al (2015) find, hard forks in practice require near-unanimity. Since this is relatively difficult to obtain, these are usually avoided. However intransigent factions that feel that diplomacy is no longer an option, or that they are being censored by the core developers, may resort to a hard fork. In this case, the threat to the initial network depends on whether a non-negligible percentage of users, value, and miners/stakers follow along with the rebellious fork. Since most cryptoasset projects are either currencies or platforms (which are generally subject to network effects), they do not easily coexist. Since widespread acceptance among both users and merchants is required for a currency to function,

it's difficult to imagine a world in which multiple similar virtual currencies achieve widespread usage. However, if these currencies fulfill different use cases, they could exist side by side. For instance, if bitcoin comes to predominate, and remains transparent, it could exist alongside a fully anonymous currency that penetrates into markets bitcoin cannot. The chief factor determining whether a cryptoasset is a competitor to another is the similarity of their use-cases; hence a fork with few modifications is a threat to the parent network.

Since it's costless to copy and paste code, under an open source license, forking is common. Most of the hundreds of projects in existence today can be traced to a handful of initial projects. That is part of the reason there has been such an incredible proliferation of cryptoassets since bitcoin was created – most of them tweak one or two parameters slightly to see how they'd work in the wild. Due to network effects, most of the value stays within a select few projects. However, worries about bitcoin's future and scaling led to an explosion of altcoins in spring 2017. As far as forks go, Bitcoin has weathered repeated alternative implementations led by competing developers. Some examples include BitcoinXT, Bitcoin Classic, Bitcoin Unlimited, and Bitcoin Cash. They all sought to increase throughput by altering a crucial parameter – the size, in megabytes, of the 10-minute blocks which compose the blockchain. This was strongly opposed by the core developers, and so advocates angling for a blocksize increase resorted to forks.

On August 1, developers behind Bitcoin Cash carried through on their promise of duplicating the chain. This was framed as a competitor to the Bitcoin protocol, and the developers behind Bitcoin Cash appealed to Satoshi's (the original bitcoin author) "original vision" (Bitcoincash.org, 2017). Hence it was clearly intended to compete with Bitcoin, in the process splitting up the network.

The competitive positioning and intended use-case is crucial in differentiating neutral airdrops from "hostile spinoffs". Few bitcoiners saw Clams or Stellar or Byteball as direct competitors, and few bothered to collect their dividend. However Ethereum Classic and Bitcoin Cash both posed a more serious threat to the parent networks, being framed by the developers as the "true" chain, with the forked source code remaining almost identical to the original. These can be thought of as hostile spinoffs. Neutral airdrops, on the other hand, provide holders of the reserve currency (bitcoin, thus far) with periodic passive income.

2. Poorly acquisitive

Open source networks, lacking corporate structure and binding developer agreements, cannot be acquired. Intellectual property is generally nonexistent, aside from open-source licensing constraints. The vast majority of open source projects boast no physical assets. While open source projects are generally donor-funded, these are managed in many cases by foundations (De Laat, 2007). Hence acquisitions are largely foreign to the space. Since these open-source projects generally focus around incentivizing a network to adopt their platform, they are poorly transferable. And they are often created in specific opposition to the perceived dominance of corporate closed-source software (Franck & Jungwirth 2003), and so a corporate acquisition of an open source network would be rejected by the community. Even if the key developers of a project were hired by an organization benefiting from the technology, as commonly happens, the project retains a non-corporate identity.

Acquisitions do occasionally occur, labeled coin swaps. The difference between a coin swap and a codebase hard fork is subtle – the former is done with the asset of the tokenholders being acquired, the latter involves copy-pasting existing code and attempting to coax an existing community to the new project. Swaps generally involve maintaining the existing blockchain, while "repository forks" take existing code and relaunch it under a new name, with the old tokenholders receiving no preferential treatment. Given the difficulty involved in benignly commandeering an existing community or token, repository forks are more common than coin swaps.

One such example is the Monero launch: the community disagreed with the incentive structures of the parent coin (it was alleged that the Bytecoin founders had secretly mined vast quantities of coins (Bitcointalk.org, 2014)[4]), and moved *en masse* to the new project, albeit with a nearly identical codebase. So while acquisitions do occasionally occur, they are rare with functioning, actively developed networks, and are only more common with zombified projects.

3. Non-dilutive fundraising

Due to established securities law, almost no tokensales have offered blockchain-based *equity* in their companies. Instead, tokens are either a pre-sold access key to a future service, or a

[4] Note: The author makes no determination as to the accuracy of the anonymous post on bitcointalk.org but it has been read over 96,000 times and so the allegations are mentioned here.

valueless investment tied in some nebulous way to the success of the platform. Crypto-tokens, in the vast majority of cases, do not imply ownership of the platform, a claim to cash-flows of the underlying, or indeed carry any governance rights. Developers can promise some capital-return mechanism to token-holders, but these are not legally enforceable. Thus most tokensales are structured not as equity purchases (as developers rarely seek to register with local securities regulators) but rather as contributions or donations, often to a foundation. For instance, the Tezos tokensale, which raised $232 million, involved contributors making a donation to the Tezos Foundation, based in Zug, Switzerland. These tokens will grant token-holders voting rights over the protocol but no legally enforceable governance rights over the foundation or the closely-affiliated Delaware company, Dynamic Ledger Solutions.

Thus developers issuing tokens in crowdsales can pursue the joint fundraising strategy of soliciting contributions from global cryptocurrency investors while simultaneously raising capital for their private companies in their local jurisdictions. This has the potential to introduce perverse incentives into the system, as the funds raised come with no legally binding obligations on the part of the founding team. This dramatically raises investor risks, but has not tempered their enthusiasm for this novel asset class.

4. Single-shot fundraising

Few token sales provision for future fundraising rounds; since token scarcity is advertised to investors, subsequent dilution is rare. While newer ICOs like Filecoin have operated a dual fundraising structure, selling $52m to pre-ICO investors and then roughly $200m to retail investors at the ICO stage, fundraising is generally a one-time enterprise. It is common for tokensales to allocate 100% of the tokens that will ever exist on a network to some combination of developers, ICO investors, early investors, foundations (for long-term funding). Private companies courting venture capital undergo multiple rounds of funding at different valuations, but the majority of tokensales only have a single initial valuation. This loss of flexibility has serious implications for investors and the tokenized networks themselves.

Single-issue fundraising forces founders to make an accurate guess as to the value of their network or protocol, prior to its launch. Tokensales generate exit opportunities for early supporters, even while no product exists, generating perverse incentives. They are conceptually similar to IPOs, while the underlying protocol more closely resembles early-stage tech startups. Hence venture-capital models of valuation are more appropriate. This poses serious risks for

retail investors who cannot achieve meaningful diversification and thus could be wiped out by the failure of a single token.

Additionally, tokens raised carry no obligations for founders, although in some cases they self-impose vesting schedules. Since the fundraising typically enables developers to build, scale, and financially support the network, its effectiveness is unknown until the development process is completed and it launches. This raises risks in both the aggressive and conservative fundraising scenarios: if developers are optimistic, and the network ultimately produces less value than the tokensale predicts, the tokens purchased by investors might decline in value; if the market undervalues the network, developers may be insufficiently compensated relative to the scope of the project. And instituting price stability or discretionary monetary policy requires the delegation of a large percentage of tokens to the development team; which implies a necessary centralization. The single-issue token model is thus poorly flexible and not well-optimized for incentive alignment.

III. The importance of decentralization

Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

– **Satoshi Nakamoto, 2008**

Censorship Resistance

Decentralized networks became viable with the mass adoption of the internet. The most successful efforts involved file-sharing on networks like BitTorrent or eDonkey. In 2016, peer to peer file-sharing accounted for 9.1% of global consumer internet traffic, according to Cisco (2016, updated 2017). The popular Pirate Bay file-sharing network survived for years in a hostile legal environment by routing traffic through cloud-hosted servers in a variety of jurisdictions. The file-sharing itself is conducted on a peer-to-peer basis. However the service was beset by multiple legal challenges and police seizures. This demonstrates the futility of decentralization at the protocol level if centralized leadership is required. Despite the Pirate Bay's struggles, decentralized file-sharing remains a popular way to share copyrighted information.

The anonymous Tor browser is another peer to peer network used by individuals seeking to obfuscate their online activities. Its decentralized and voluntarist leadership structure has seen it maintain continuous development since 2002, even though it a (passive) enabler of illegal activity, among other things. Tor's decentralized node and leadership structure has made it impossible to shut down. If the US government were to raid the offices of the Tor nonprofit in Massachusetts, its open-source code could be forked and relaunched elsewhere. Some of its developers are not US-based, and could therefore contribute without recriminations. Since participants on the Tor network serve as nodes on the network, and the network enjoys a popular userbase, global traffic can be routed with low latency regardless of origination.

Thus networks find resilience in their decentralization of nodes, distributed and non-hierarchical leadership, and open-source development. Decentralized networks enable global interaction between disparate parties in a way that cannot easily be controlled or inhibited by governments or large corporations. This feature is commonly known as censorship-resistance.

Censorship-resistance was a defining motivation for the Bitcoin software protocol, as explained in Satoshi Nakamoto's introductory online post:

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. (Nakamoto, 2009)

Peer to peer currency enables individuals to exchange and hold value independent of the conventional central banking system. Monetary policy is algorithmic and predictable. A "distributed system with no single point of failure" (Nakamoto, 2009) cannot easily be shut down. It would be difficult for a governmental to successfully attack Bitcoin today; it would require a coordinated global effort to shut down the tens of thousands of nodes running the software.[5]

Bitcoin is not perfectly censorship-resistant, as individuals depend on exchanges to obtain the virtual currency, mining activities are heavily concentrated, and a few corporations employ the most important developers. However, its global nature, prohibitively expensive cost to attack,

[5] This refers to a hashpower-based 51% attack; the Chinese government could mount an extra-protocol attack on Bitcoin with simultaneous mining operation raids, as a large fraction of miners are based in China.

dispersion of nodes, and largely voluntarist developer community render it resilient to most attacks, be they technical or political.

Dis-intermediation and the elimination of third parties

Decentralized networks like Bitcoin enable transactions to occur between individuals with no centralized bank required to ratify them. Instead, these transactions throughout the network, and if valid, they are ratified by participating network nodes. Assuming that no cartel or individual player controls more than 51% of the network hashpower, the network's ratification is assumed to be a faithful approximation of the history of transactions. While miners are under no obligation to follow the rules of the protocol, or to honestly ratify transactions, their signals are rejected by the network if they do not align with the majority of hashpower. And since they are paid in the currency tied to the protocol, miners are incentivized to support and grow the network.

This innovation enables trustless transactions between potentially adversarial parties. The work of a bank is outsourced to a global network of peers. Assuming transactors pay sufficient fees to incentivize the network to accept their transaction, these transactions are, after a brief period of time, sound and irreversible. This has significant benefits from merchants, who no longer risk the uncertainty of a credit transaction being revoked. Many merchants accept bitcoin transactions at a discount to typical ones, as they ascribe a premium to irreversible payments.

Digital currencies also enhance certainty and convenience across jurisdictional boundaries. This extends to use-cases like remittances, which do not require central parties like Western Union to intermediate payments (although conversion to fiat does require on and off-ramps). A significant industry has emerged to facilitate these sorts of bitcoin transactions. While centralized services like Venmo and Paypal are superior in convenience, speed, and transaction costs, these do not possess the censorship-resistance or multi-jurisdictional qualities of bitcoin. One of bitcoin's earliest successes saw holders of the digital currency use it to contribute to Wikileaks in 2011 (Popper, 2015), when the leaks service was blacklisted by most financial institution. More trivially, Venmo does not function across international boundaries, and doesn't exist in foreign jurisdictions. Bitcoin is a way to circumvent both of these problems.

More broadly, distributed ledgers are touted as a means to dis-intermediate a variety of functions outside of the financial industry. Any industry which has transaction costs, third party frictions, significant notarization costs, or clear inefficiencies is targeted for disruption by

startups aiming to use distributed ledge technology. These novel protocols are intertwined with tokens to generate network effects, incentivize participants to use the product once it is released, fund developers, and to generate the economic incentives that secure the networks. While distributed networks do not need to be tokenized to function (see Tor or BitTorrent), the additional token layer injects explicit economic incentives into the system. It is this combination of distributed networks and the tokenization that yields these popular entities launched through token sales or Initial Coin Offerings.

In these cases, political resilience is not the main goal, but rather the dis-intermediation of centralized services, the creation of efficiencies, or the tokenization of illiquid assets. For instance, Steemit incentivizes users to create worthwhile social media content by enabling users to allocate STEEM to quality posts (thus rewarding content creators). Basic Attention Token, in coordination with the Brave browser, introduces efficiencies into online advertising by transparently quantifying the attention users give to advertisers. Golem aims to commoditize spare processing power by creating a decentralized market for graphical processing. Thus while not every token is politically motivated, they generally aim to resolve an inefficiency, dis-intermediate services, or create a market for a previously illiquid good.

Avoiding the 'Security' moniker

This is an object of crucial, if secondary value. While cryptoasset trading is global, a huge fraction of startups, founders, institutional participants, investors, developers, and exchange volume is based in the US. This exposes the industry to American securities law. Additionally, decisions made by the SEC tend to have global knock-on effects, as regulators imitate US laws. American regulators have been making their presence felt on a global basis, recently arresting a Russian national in Greece for running an exchange that laundered stolen bitcoins (Popper, 2017). American law enforcement collaborated with European partners to close down a darknet bitcoin-based market based in the Netherlands, and arrested the Canadian founder of another darknet market in Thailand (Popper and Ruiz, 2017). American regulators and law enforcement are not afraid to exert their influence on a global basis.

Nascent distributed applications therefore have a very strong incentive to comply with US securities regulation. While political decentralization alone doesn't guarantee that an asset would not be labeled a security under the Howey test, it is one means of avoiding the damaging security label. It could be argued that the enthusiasm for recent ICOs is due in part to the

untethering of the process of raising early tech capital from the closed ecosystem in Silicon Valley. Tokens exposed developers to a global audience of tech-savvy investors with money to spare (after bitcoin and ether generated $100 billion in investor value). This alternative capital market has yielded investors eye-watering returns, yet these can be conceptualized as compensation for the substantial risks incurred. These include the risk of total expropriation of funds invested by developers or founders; technical difficulties or the complete failure to launch a platform; no investor protection from arbitrary dilution; the risk of investing in a shell token; and immediate liquidation after fundraising and project abandonment.

Governance decentralization is one means of avoiding being branded a security. In the SEC memo on The DAO, the decentralized Bitcoin protocol and the Ethereum distributed computing platform were considered not to be securities. Brito and Castillo (2016) note that distributed, not centrally-controlled platforms such as Bitcoin and Ethereum "do not easily fit the definition of a regulated security," in contrast with "centrally-organized and questionably marketed" tokens. Brito and Castillo were proven right as the SEC subsequently labeled the centrally controlled DAO (with only perfunctory tokenholder governance; and administered by Slock.it) an unlicensed security, but exonerated Ethereum itself.

Therefore decentralization has value in maintaining censorship resistance, dis-intermediating trusted third parties and resolving inefficiencies, and more pragmatically in designing a compliant protocol. However, the term itself has been the subject of considerable debate, and it too, deserves clarification.

Dimensions of decentralization

It is often assumed within cryptoasset communities that decentralization is univariate; i.e. it is satisfied if network nodes are geographically distributed. This follows from a narrow technical analysis of distributed systems. In a system where the cost of running a node (as measured by bandwidth and storage requirements) is inversely proportional to the number of users willing to run a node, node decentralization can be quantified through node cheapness. This is the position advocated by Bitcoin developer Paul Sztorc (2015b). However nodes alone do not ensure that a distributed protocol is decentralized. A decentralization analysis must incorporate power structures. Gervais et al (2014) lend credence to this view, finding Bitcoin's decentralization lacking in decision-making, mining, and incident resolution. Srinivasan and Lee

(2017)[6] sketch an informal model of decentralization in cryptoassets, finding Gini coefficients for six parameters: mining, exchanges, clients, developers, nodes, and ownership. This captures some but not all of the qualities of decentralization. In particular, it is infeasible to quantify extra-protocol power structures. Additionally, exchanges are exogenous to currency dispersion; some segregation among exchanges is necessary,[7] but in the current vibrant exchange environment, this follows naturally for quality projects. And regulated exchanges at present pose little threat to their currencies.[8] Additionally, in a PoW system, ownership is immaterial, as tokenholders have few or no rights. And pure node dispersion is specious; it's trivial to initiate dozens of nodes on cloud servers – true node decentralization is a function of the ability of individuals in a variety of settings to run them.

I find it more useful to trace power relationships and order decentralization on that basis. A truly decentralized system is characterized by decentralization at the node, miner/staker, and governance level. While this model flows logically from an analysis of power structures typified in the bitcoin model discussed in this paper, theoretical support comes from Schneider (2003). Schneider, responding to conceptual confusion in academia over political decentralization, finds that decentralization is political, administrative, and fiscal. Within the Bitcoin network, decision-making structures (chiefly orchestrated by Core developers) can be understood as political, nodes enforcing rulesets can be understood as administrators, and fiscal power is wielded by miners. Since miners engage in the largest investments of economic resources into the network, they can be seen as fiscal guarantors of the system. While the analogy is imperfect, Bitcoin's segmented power structures lend themselves to a multivariate analysis.

Critics may contest my analysis of Bitcoin as political. However the protocol itself is a clear answer to a political problem – how to create a stable monetary system outside the purview of central banking – and distributed networks more generally are an effort to wrest power from central authorities. Distributed systems carrying billions in economic value require decision-making, especially those consisting of software requiring updates. The process of making

[6] Srinivasan is the CEO 21.co, one of the largest and earliest recipients of venture-capital funds in the Bitcoin industry.
[7] The hack and failure of the Mt Gox exchange in 2014 plunged Bitcoin into a two-year bear market and destroyed confidence in the currency; at the time Mt Gox accounted for 70% of exchange volume.
[8] When exchanges are cut off from banking and resort to alternative funding methods however, they do pose a threat to the underlying assets. This is the case with Bitfinex today.

decisions in inherently political, and a system must be chosen, even if it an emergent and uncodified one.

Hence I model decentralization along three dimensions: political (governance-level), protocol level, and node-level. This analysis holds for Proof of Stake projects as well, with stakers replacing miners at the protocol level. A select few projects condense the protocol and governance layers into one, but the vast majority exhibit this three-tiered structure. Features are summarized in *Table 1*.

Dimensions of decentralization in distributed networks

	I. Political	II. Protocol	III. Node-level
Decision-making scope	Top level, extra-protocol rules	Intra-protocol decisions	Transaction validity, software clients
Chief participants	Founders, developers, leaders	Miners, stakers	Participating computers
Characterised by	Dispersion of decision-making power	Dispersion of miner hashpower/staking tokens	Cheapness and proliferation of nodes
Measurability	Difficult, often poorly codified	Moderate, anonymous participants	Trivial
Decentralization requirement	Necessary but not sufficient	Necessary but not sufficient	Necessary but not sufficient
Commonness in popular projects	Rare	Common but not universal	Near universal
Ideal paradigm	Meritocracy, public delegative democracy	No miner or staker with more than 5% of distribution	Large number of cheap and distributed nodes

Table 1: dimensions of decentralization

These multiple decentralization variables have a practical use: they introduce political centralization as a key risk factor for investors. Mere node-decentralization is insufficient for a truly decentralized protocol; the protocol and governance must be considered. It's worth noting that decentralized decision-making is directly traded off against efficiency of decision-making. This makes decentralized governance undesirable for projects seeking to develop quickly and gain market share, but desirable for other reasons – obtaining community legitimacy and escaping regulatory crackdowns. Truly decentralized governance is rare in the asset class, and may ultimately be incompatible with the rigors of running an actively developed software project.

IV. Empirical results

Methodology

Key empirical results consist of a cross-sectional survey of the most popular cryptoasset projects. Novel data on governance, funding methods, project structure, and other investor risk factors is presented. Qualitative data was collected over a three-month period, although

quantitative data points reflect a snapshot taken on July 29, 2017. The cut-off date for new asset inclusion into the list was also July 29, so newer ICOs are omitted. Data on distributions was collected through a reading of white papers, investor prospectuses, and legal disclosures. Descriptions were assigned according to the taxonomy presented in this paper. Data on launch methods, developer funding models, governance models, and red flags was found through an ethnographic investigation of diverse sources stretching from community forums to direct interviews with founders and developers. Developers and founders who were questioned were given the chance to opt-out of the conversation and were informed of the purpose of the study.

The inability to easily procure meaningful information was noted, manifesting itself in the transparency column. Information on open source projects was taken from CoinGecko's aggregation, and project pages on Github. Funding and governance models were determined from an analysis of public information provisioned by these projects, although they were frequently obscured and nonpublic. Governance models are assigned according to the methodology discussed in this paper. Algorithm and quantitative information is taken from the CoinGecko, CoinMarketCap, BraveNewCoin, and Smith+Crown information aggregators. Corporate and foundation affiliations were extracted from an analysis of legal disclosures, a survey of founder LinkedIn pages, and company registration directories. The information included in the survey is publicly available, if difficult to obtain. Cryptoassets at present are largely unregulated and not subject to insider trading or disclosure rules.

Variable explanations

Network value. This is a figure structurally but not conceptually comparable to "market capitalization" of a stock – it multiplies token value by the number of outstanding tokens in circulation. Figures are taken from a snapshot of CoinMarketCap on July 29, 2017. While network value is not a reliable way to determine the value of a network, due to widely varying floats, it is a commonly used figure and hence employed here. The selection is arbitrary due to the trivial manipulation of network value on aggregators like CoinMarketCap. That said, the sample was appropriate for the study since it usefully includes some "shell" networks – those with a high network value and little development activity or community. This meant that the cross-section includes a variety of projects and governance models. Finally, while network value is a poor approximation of actual value, many investors perceive it as such and so this lens views the market from the perspective of a typical retail investor. It's important to note that this is not a representative sample, as many hundreds of cryptoasset projects exist (and many more

are defunct). This exposes the study to survivorship bias. The sample is selected to demonstrate investor risk by including the most visible projects. Since network value can be exploited by some promoters to grant visibility to their project, this survey of the projects with the highest network values includes both the largest and most mature projects, as well as some shell tokens. This yields a useful heterogeneity of features.

Average daily volume. Figures come from CoinMarketCap on July 29th. Average daily exchange volume is obtained by averaging the volume of the previous thirty days. Note that CoinMarketCap includes volume figures from untransparent and small exchanges which may host fee-less trading, so volume figures are also trivially manipulated.

Launch style. "Fair" launches imply that the launch was announced publicly, with the coin mineable from the start, with parameters that made it open to anyone. These are limited to PoW coins. Fair launches are few, as they exclude those coins which have been premined by creators. Siacoin is listed as fair as the premine represented a mere 0.09% of all outstanding coins. ICOs refer to initial coin offerings or token sales, and they typically involve founders selling some percentage of existing coins to investors in a tokensale occurring over a matter of days or weeks. Founders often keep a cache of coins behind so that they can fund further development; this is listed in the "founder reserve" column. Instamines and stealth mines involve the release of a coin, but with a degree of subterfuge; in those cases, founders used asymmetric advantages to mine large percentages of the coin at launch or failed to announce the inception of the coin, thus mining stealthily. Hard forks occur when a section of the community contests a decision and implements new rules that are incompatible with the previous blockchain history, thus creating a new blockchain with a shared history. This was how Ethereum Classic was launched. Lastly, airdrops occur when founders borrow the distribution of an existing network – usually bitcoin – to guide distribution of a new currency. This the bitcoin ledger is transparent, airdrops are a common tactic to distribute new tokens in a fair and transparent manner.

Created at launch. This column refers to the percentage of tokens brought into existence when the networks were first created. Proof-of-stake tokens are not secured by mining, and are typically not inflationary, so they often have 100% initial creation schedules. This means that the initial distribution is a determinant of who holds future power in the network, especially if the

tokens allow voting mechanisms. In a PoW system, a high initial creation percentage is another red flag, as typical fair launches start from zero.

Founder reserve. This is the percentage of tokens controlled by founders. Tokens that were fairly mined by founders (such as Satoshi's estimated 1m bitcoins) are exempt, as they were not costless to acquire. Percentages are a function of outstanding tokens as of July 29. For instance, 12m ether were reserved at launch for developer salaries, in addition to the 60m sold in the presale. Today there are 93.9m ether outstanding, meaning that the 12m reserved for developers account for 12.7% of the outstanding tokens. Higher founder reserve percentages, or obscure and non-public reserves, imply more potential for rent-seeking activities.

Corporate support. This variable details the corporate entities backing the projects on the list. In some cases, developers are all contracted to a corporation, which controls every aspect of the network. In others, corporations employ a selection of top developers, in which case it is listed as affiliated. Instances where developers are heavily linked with a corporate client are listed as partnerships. Except for particular notable jurisdictions, country names and two-letter US state codes are used. Registration addresses are used, where known. For instance, the Stellar Development Foundation is located in San Francisco, but registered in Delaware, so the latter is used.

Developer funding. This variable isolates how the developers are paid. Primary funding methods are listed first. The Bitcoin protocol, for instance, is developed on a mostly volunteer basis, although many top developers are employed by organizations who benefit from the protocol, so the funding model is listed as volunteer/corporate. "Token reserve" is a funding model in which tokens are controlled by a corporate, charitable, or other entity and periodically sold off to pay developer salaries. "Corporate" or "foundation" based funding denotes a model in which a large percentage of funding comes in the form of salaries and not token sales. "Community bounties" are a common method whereby projects are nominated by the community and prizes are paid to developers that successfully complete them. This is closely linked to the donor model. "Block reward fees" are another method in which a portion of each mined block is paid to developers – in the case of Zcash, this is 20%. Miners consent to this because developers add value to the project. Siacoin has a similar structure, in which a percentage of each contract for storage goes to the parent company which employs developers.

Foundation. Whether one exists, and where it's registered.

Governance model. This category has some ambiguity involved, as extra-protocol governance cannot easily be determined for many projects. The vast majority have implicit and unstated governance structures. The question in determining the model was "who ultimately makes decisions over the system?" Much of the time, this was a matter of determining who controls funding, or who arbitrates disputes. For projects with stated governance, the actual implementation of these governance models was considered. Several projects grant tokenholders limited rights but ultimately vest power with founders. There is a common conflation between decision-making on the hardcoded algorithmic rules of the system, for instance by miners, and ultimate decision-making structures over key decisions, like expenditures, the settlement of disputes, and the assignment of developer power. This category refers to the latter: extra-protocol governance. In cases where this governance is subsumed into the protocol itself, this is mentioned; although these efforts are new and hence rare. Many projects have made promises about assigning rights to stakeholders; few have delivered.

"Open" implies a meritocratic, non-hierarchical, reputation-based system. "Core consensus" is a system in which consensus is obtained primarily from a small group of developers. Foundation or corporate models delegate power primarily to those entities. "Delegated tokenvotes" are a system in which token holders elect representatives, not for propositions directly. "Masternodes" see power concentrated in the operators of a special class of nodes (which require significant token ownership) rather than all tokenholders. Miner-based systems are ones in which miners have some control over the system. The primary model is listed first.

Defined governance. Partially defined governance refers to a situation where some aspect of governance is codified, but other power structures are left unstated. In Bitcoin, the process of proposing and debating improvements to the network among developers is structured and codified; however, the process of implementing these changes or arbitrating disputes among miners and nodes, and in the case of competing hard forks, is not formalized. So governance is partially defined. Planned governance is a feature of projects that have committed to returning power to tokenholders but have not yet released full details or an implementation.

Public developers. Some projects have fully anonymous development teams, and indeed in some privacy-oriented communities this is presented as an advantage against a coordinated

attack. The nature of open source means that diffuse and nonpublic developer teams can collaborate productively. However, some investors are wary of committing funds to a project with nonpublic developers.

Transparency. Cryptoasset projects are deemed to have good, fair, or poor transparency based on some simple features. While there is inevitable subjectivity in these judgments, the methodology is straightforward and replicable. Good transparency is characterized by openness about corporate and foundation backers for the project, and their jurisdictional registration; clearly defined issuance mechanisms, including the percentage of tokens held by founders and inflation rates; detailed descriptions of how raised funds will be spent; periodic blog posts during development; clear responses to investor queries; and well-defined token uses.

Poor transparency is characterized by projects with unclear corporate backers and evasiveness about registration; censorship in the forum, or a lack of a public forum entirely; nonpublic slack groups, or bans from slack groups when questioned; infrequent or no development updates; unclear launch and token issuance mechanisms; unclear token distributions to founders; non-public founders and promoters; and deliberate over-complexity or obfuscation in the governance, launch, or corporate structure of the project. Fair transparency is the middle ground, although outright censorship and an inability on the part of founders to provide meaningful answers ruled out anything other than a rating of “poor.” I draw upon Van Valkenburgh’s (2016) methodology for grading transparency in distributed token networks here.

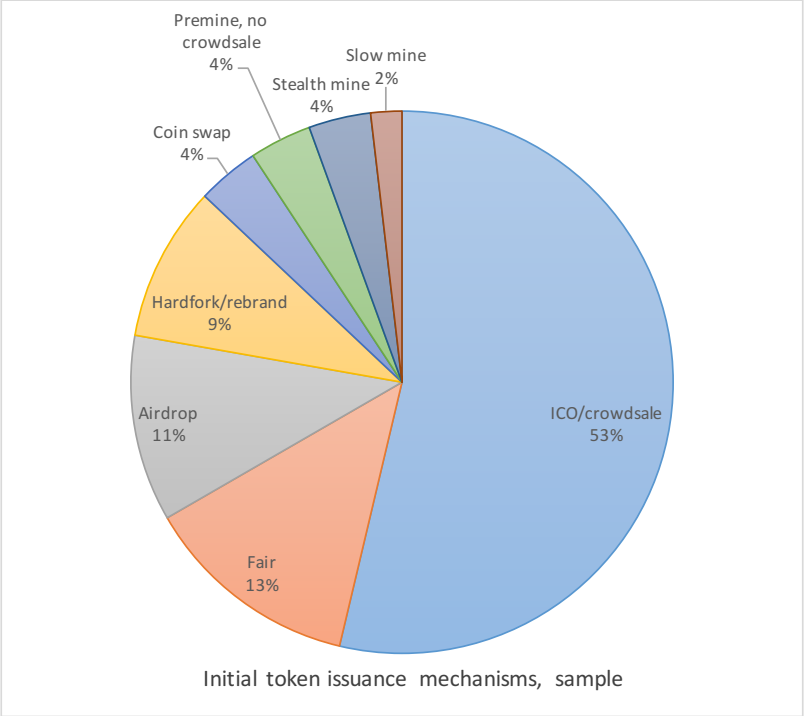
Open source. This is a more binary variable detailing whether project code is available for public scrutiny, or kept proprietary. Some corporate projects seek to maintain control over intellectual property, and so do not release open-source code. Others release only cursory amounts and have inactive Githubs. Some projects are still developing an alpha release and have closed-sourced development until then, so they may open-source development in the future.

Presentation of results

In *Tables 2* and *3*, survey results for the top 50 assets by network value are presented. Taken together, these dimensions present a qualitative analysis of developer incentives, corporate structures, funding models, and decision-making processes for a large set of projects. Much of

the analysis is qualitative, and so is ill-suited to regression techniques, although more work in this domain would be welcomed. Some conclusions can however be drawn.

Figure 2, token issuance mechanisms

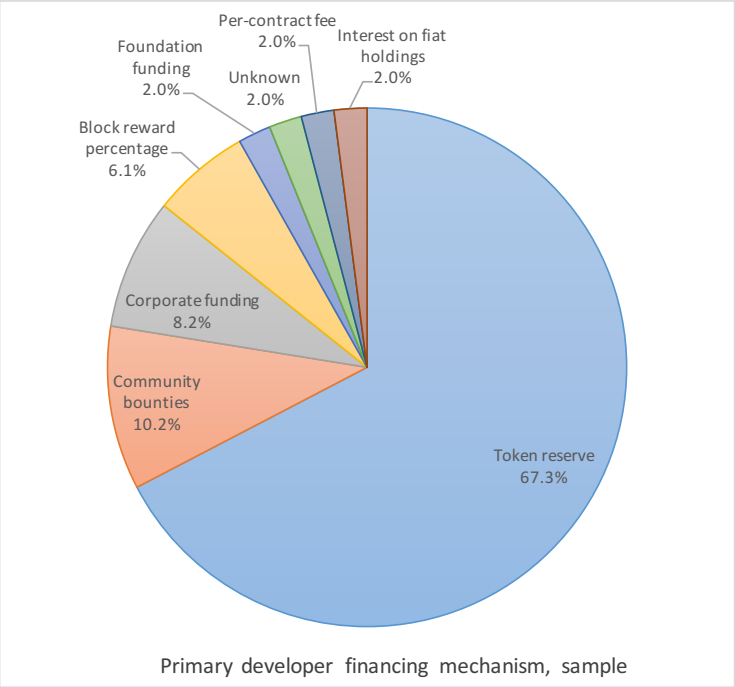


The survey confirms the immense popularity of Initial Coin Offerings or tokensales as a distribution method among popular projects, as 53% of the projects surveyed follow this distribution model (see *Figure 2*). Maintaining a token reserve to pay developers was even more popular, as 67% of the projects used that as their primary funding model (more detail in *Figure 3*). Community bounties were also popular, representing 10% of the sample. Developer financing is heavily concentrated in token reserves, which poorly align founder incentives with measures of network success like transaction load and liquidity; but are rather a function of network value. Pure play cryptocurrencies were not quite as popular as platform tokens in the sample. Only a select few projects had a “fair” initial distribution, were mineable, and had no corporate sponsors. From the sample, appropriate founder reserves are inferable; the mean being 19.68% and the median resting at 15%.

Perhaps the most surprising conclusion from this sample is the near-ubiquity of direct corporate influence on these projects. The startup model is ill-fitted to FOSS networks, as funding is single-shot, development is typically open source (and can be forked away from the company), community consensus can be discarded, and central agents issuing tokens risk violating securities law. Despite this, the vast majority of projects had either a direct corporate entity exerting control over developers and funds, or close corporate affiliates.

Figure 3, primary developer financing mechanisms

Another startling feature of the ecosystem is the distinct lack of transparency among many projects. Some exhibit closed-source development, which is antithetical to the original nature of free open source networks. Transparency, according to the scale employed, is generally poor, even though cryptoasset projects are relied upon for voluntary disclosure at present, since no specialized regulatory requirements exist. The occasional closed-source development, ubiquitously poor transparency, and the presence of corporate funding and control, all imply that the ecosystem is doing a poor job of self-regulating.



Primary developer financing mechanism, sample

Table 2, cross-sectional survey, part I

Name	Consensus mechanism	Description	Network value, m	Daily vol, m	Launch Style	Created at launch	Founder reserve	Mineable	Corporate support
Bitcoin	PoW	Cryptocurrency	$ 45,037	$ 1,039.3	Fair	0%	None	Yes	Core devs affiliated with Blockstream (Montreal)
Ethereum	PoW	Platform (smart contracts)	$ 18,354	$ 998.3	ICO	77%	12.7%	Yes	Affiliated with Enterprise Alliance (multiple)
Ripple	n/a	Settlement system	$ 6,357	$ 122.2	Private sales	100%	20%	No	Ripple labs (San Francisco, CA)
Litecoin	PoW	Cryptocurrency (fast/cheap transactions)	$ 2,135	$ 355.2	Fair	0%	None	Yes	n/a
NEM	PoImportance	Platform	$ 1,497	$ 4.2	ICO	100%	28.9%	No	Affiliated with Tech Bureau Inc. (Japan)
Dash	PoW/PoS	Cryptocurrency (privacy)	$ 1,337	$ 44.9	Instamine	26% (disputed)	Unclear % of instamine	Yes	n/a
Ethereum Classic	PoW	Platform (smart contracts)	$ 1,313	$ 144.2	Airdrop/hard fork	0%	None	Yes	IOHK (HK), Greyscale (NY)
IOTA	DAG/PoW	Platform (microtransactions)	$ 748	$ 5.0	ICO	100%	5%	No	Affiliated with Jinn Labs (unknown)
Monero	PoW	Cryptocurrency (privacy)	$ 655	$ 13.1	Fair	0%	None	Yes	n/a
Stratis	PoW/PoS	Platform (enterprise blockchains)	$ 501	$ 10.9	ICO	100%	14%	No	Stratis Group Ltd (U.K.)
EOS	DPoS	Platform (smart contracts)	$ 444	$ 92.1	ICO	100%	10%	No	Block.one (Cayman islands)
BitConnect	PoW/PoS	Cryptocurrency (lending/referrals) (shell)	$ 412	$ 3.0	ICO	17%	Unclear	Unclear	n/a
NEO	Byz. fault tolerance	Platform (smart contracts, financial)	$ 360	$ 19.6	ICO	100%	50%	No	Onchain (Shanghai)
Bitshares	DPoS	Platform (asset exchange)	$ 349	$ 30.0	Airdrop, ICOs, swap	Unknown	Unknown	No	Invictus Innovations Inc. LTD (HK); Cryptonomex Inc. (VA)
Zcash	PoW	Cryptocurrency (privacy)	$ 336	$ 24.3	Slow-mine	0%	None	Yes	Zerocoin Electric Coin Company (CO)
Qtum	PoS	Platform (smart contracts, UTXO)	$ 331	$ 13.8	ICO	100%	20%	No	Affiliated with Bloqlabs (Chicago, IL)
Tether	n/a	Fiat pegged token (shell)	$ 319	$ 118.8	Exchange issue	Unclear	n/a	No	Tether Ltd (HK) Tether Holdings Ltd (Cayman), iFinex, Inc (HK)
Steemit	DPoS	App token (content creation)	$ 304	$ 1.9	Stealth mine	75%	Unknown	Initially	Steemit, Inc (NY)
Veritaseum	Unclear	Platform (capital markets) (shell)	$ 301	$ 1.3	ICO	51%	98%*	Yes	Veritaseum Inc (NY)
Waves	Leased PoS	Platform (token creation)	$ 290	$ 2.4	ICO	100%	15%	No	Unclear incorporation (Russia)
Iconomi	n/a	Platform (asset management)	$ 262	$ 1.8	ICO	100%	15%	No	Iconomi Inc (St Vincent), Cashila o.o.d, Slovenia
Siacoin	PoW	App token (storage)	$ 235	$ 11.4	Fair	0.09%	<1%	Yes	Nebulous Inc. (MA)
Tezos	DPoS	Platform (smart contracts, governance)	$ 232	$ -	ICO	100%	18.5%	No	Dynamic Ledger Solutions (DE)
Bytecoin	PoW	Cryptocurrency (privacy) (shell)	$ 224	$ 1.3	Stealth mine	82%	Unclear	Yes	Various affiliated companies, unclear
Gnosis	n/a	App token (prediction market)	$ 213	$ 2.2	ICO	100%	95% (10% founders)	No	Gnosis Limited (Gibraltar), Consensys
Lisk	DPoS	Platform (sidechains)	$ 206	$ 4.1	ICO	100%	7.3%	No	n/a
Dogecoin	PoW	Cryptocurrency (tipping, charity)	$ 193	$ 6.5	Fair	0%	None	Yes	n/a
Golem	n/a	App token (decentralized computing)	$ 191	$ 4.3	ICO	82%	18%	No	Golem Factory GmbH (Zug)
Augur	Reputation based	App token (prediction market)	$ 190	$ 3.0	ICO	100%	20%	No	Partnered with Microsoft (WA)
Stellar Lumens	n/a	Money transfer (global financial access)	$ 183	$ 10.4	Airdrop	100%	83% (dist. ongoing)	No	n/a
Status	n/a	Mobile client (ethereum)	$ 178	$ 19.8	ICO	100%	20%	No	Status Research & Development Gmbh (Zug)
Factom	Federated consensus	App token (data verification)	$ 155	$ 3.5	ICO	13%	4%	No	Factom Inc (TX)
Decred	PoW/PoS	Cryptocurrency (governance)	$ 153	$ 1.4	Airdrop/premine	28%	14%	Yes	Company 0 LLC (IL)
DigiByte	PoW	Cryptocurrency (multi-algorithm)	$ 150	$ 8.6	Premine	1.2%	0.6%	Yes	DigiByte Holdings Ltd (Hong Kong)
Byteball	DAG	Cryptocurrency (conditional payments)	$ 149	$ 0.9	Airdrop	100%	1%	No	n/a
MaidSafeCoin	Proof of Resource	Platform (data storage)	$ 141	$ 1.7	ICO	30%	15%	No	MaidSafe Ltd (Scotland)
GameCredits	PoW	Cryptocurrency (in-game purchases)	$ 133	$ 1.9	Fair	Unclear	Unclear	Yes	GameCredits, Inc (LA), Datcroft Games Ltd. (London)
DigixDAO	Proof of Asset	Cryptocurrency (asset-backed)	$ 129	$ 0.4	ICO	100%	15%	No	DigixGlobal Pte Ltd (Singapore)
OmiseGo	DPoS	Platform (e-commerce, financial access)	$ 120	$ 8.0	Presale, ICO, airdrop	65%	29.9%	No	OmiseGO Pte Ltd (Singapore)
Basic Attention Token	n/a	App token (in-browser advertising)	$ 107	$ 1.5	ICO	100%	13%	No	Brave Software Inc (San Fransciso, CA)
Ardor	PoS	Platform (token creation)	$ 106	$ 2.4	Airdrop (NXT)	100%	Unclear	No	Jelurida BV (Netherlands)
PIVX	PoS (previously PoW)	Cryptocurrency (privacy)	$ 105	$ 1.1	Fair	0.1%	None	No	n/a
NXT	PoS/LPoS	Platform (token creation)	$ 100	$ 6.6	Crowdsale	100%	Unclear	No	Jelurida BV (Netherlands)
MobileGo	n/a	Platform (gaming in-app purchases) (shell)	$ 99	$ 0.3	ICO	100%	30%	No	GameCredits, Inc (LA)
Komodo	Delayed PoW	Cryptocurrency (privacy)	$ 98	$ 0.3	ICO/coin swap	50%	5%	Yes	Partnership with Monaize (France)
Populous	Proof of Asset	Platform (invoicing)	$ 96	$ 0.8	ICO	100%	28%	No	Populous (London)
TenX	PoW	Platform (retail payments)	$ 93	$ 2.2	ICO	51%	49% (founders 20%)	No	TenX PTE Ltd (Singapore)
Metal	PoProcessed Payments	Payment rail	$ 83	$ 3.6	ICO	60%	31% (founders 5.04%)	Yes	Metallicus Inc (DE), Metallicus Ltd (HK)
Aragon	n/a	Platform (decentralized orgs)	$ 74	$ 0.7	ICO	100%	30% (founders 15%)	No	Unclear, possible LLC
Bancor	n/a	Platform (token exchange)	$ 73	$ 6.8	ICO	100%	50% (founders 10%)	No	LocalCoin Ltc, (Israel)

Table 3, cross-sectional survey, part II

Name	Developer funding	Foundation	Governance model	Defined governance	Public developers	Transparency	Open source	Red flags
Bitcoin	Volunteer/corporate	Defunct	Core consensus/miner	Partially	Yes	Good	Yes	
Ethereum	Token reserve	Yes (Zug)	Benevolent dictator	No	Yes	Good	Yes	Contested hardfork
Ripple	Token reserve	No	Corporate	No	Yes	Fair	Yes	Fined $700,000 by Fincen
Litecoin	Community bounties	Yes (Singapore)	Benevolent dictator	No	Yes	Good	Yes	
NEM	Token reserve, masternode rents	Yes (Singapore)	Corporate/foundation based	No	No - all private	Poor	Yes	
Dash	Block reward fee	Yes (AZ)	Masternode voting	Yes	Partial public	Poor	Yes	Rebranded from Darkcoin, instamine
Ethereum Classic	Donor/corporate	No	Open/corporate	Planned	Yes	Good	Yes	
IOTA	Foundation based	Yes (Germany)	Foundation control	No	Yes	Poor	Yes	Censorship in forums
Monero	Community bounties	No	Open/consensus	Yes	Partial public	Good	Yes	
Stratis	Token reserve	No	Corporate	No	Yes	Poor	Yes	
EOS	Token reserve	No	Corporate	Planned	Yes	Poor	Partial	Yearlong uncapped ICO, developer history
BitConnect	Unclear	No	Unclear	No	No	Poor	No	Referral program, only available on own exchange
NEO	Token reserve	No	Corporate/tokenholder vote	Partially	Yes	Poor	No	Rebrand from AntShares to NEO
Bitshares	Token reserve	Yes, Netherlands	Partial voting rights; corporate	Yes	Partial	Poor	Partial	Complex and obscure distribution; unexpected dilution
Zcash	Block reward fee	Yes (DE)	Benevolent dictator	No	Yes	Good	Yes	
Qtum	Token reserve	Yes (Singapore)	Foundation & limited tokenvote	Partially	Yes	Poor	Partial	
Tether	Interest on fiat holdings	No	Corporate	No	No	Poor	No	Liquidity crisis due to Taiwanese banks, poor tethering
Steemit	Token reserve	No	Delegated witness election	Yes	Yes	Poor	Yes	Anonymous witnesses/ capital lockup incentives
Veritaseum	Token reserve	No	Corporate	No	Partial public	Poor	Partial	Got hacked, price manipulation
Waves	Token reserve	No	Benevolent dictator	No	Yes	Poor	Yes	Token censorship
Iconomi	Token reserve	No	Corporate/unclear	No	Yes	Poor	No	Unclear incorporation, forum censorship
Siacoin	Per-contract fee to Nebulous	No	Corporate/consensus	No	Yes	Good	Yes	Contemplated hardfork to fund devs
Tezos	Token reserve	Yes (Zug)	Tokenholder vote; foundation	Yes	Yes	Good	Yes	Bonus period in ICO
Bytecoin	Token reserve	No	Unclear	No	No - all private	Poor	Yes	Falsified blockchain; backdated whitepaper
Gnosis	Token reserve	No	Corporate	No	Yes	Poor	Yes	Multi-level token structure
Lisk	Token reserve	Yes (Zug)	Foundation based	Planned	Yes	Good	Yes	
Dogecoin	Community bounties, donations	Yes (CO)	Unclear, forum consensus	No	Yes	Fair	Yes	No development for long periods
Golem	Token reserve	No	Corporate	No	Yes	Fair	Yes	Developer silence and lengthy delays
Augur	Token reserve	Yes (Estonia)	Foundation control	No	Yes	Fair	Yes	
Stellar Lumens	Token reserve	Yes (DE)	Foundation control	No	Yes	Good	Yes	
Status	Token reserve	No	Corporate/planned token vote	Partially	Yes	Good	Yes	Pre-ICO sale; only 51% sold
Factom	Token reserve	Yes (UK)	Unclear/foundation	No	Yes	Good	Yes	
Decred	Block subsidy/bounties	No	Formal staked vote; corporate	Yes	Yes	Good	Yes	
DigiByte	Token reserve, corporate	Planned	Corporate	No	Partial	Fair	Yes	
Byteball	Community bounties	No	Delegated consensus	No	Partial	Good	Yes	
MaidSafeCoin	Token reserve/community bounty	Yes (Scotland)	Foundation, elected board	Yes	Yes	Fair	Yes	
GameCredits	Corporate funding	No	Corporate	No	No	Poor	No	Development stalled or closed-source
DigixDAO	Token reserve	No	Corporate (tokenvote planned)	Planned	Yes	Fair	No	Closed source development, minimal vote weight
OmiseGo	Token reserve	No	Corporate	No	Partial	Fair	No	Closed-source development
Basic Attention Token	Token reserve	No	Corporate	No	Yes	Good	Partial	Poor development transparency
Ardor	Corporate funding	Yes (Netherlands)	Corporate	No	Partial	Fair	No	Closed-source development
PIVX	Community bounties	No	Pure tokenholder vote	Yes	No	Good	Yes	Rebrand
NXT	Corporate funding	Yes (Netherlands)	Corporate	No	Partial	Fair	No	Closed-source for long periods
MobileGo	Token reserve	Yes (unclear)	Developer control	No	Partial	Poor	No	Closed source development, dual token with GAME
Komodo	Token reserve, bounties	Yes (pending)	Delegated consensus	Partially	No - all private	Good	Yes	Rebrand, private developers
Populous	Token reserve	No	Corporate	No	Yes	Poor	No	Uses virtual address in London, promises returns
TenX	Token reserve	No	Corporate	No	Yes	Poor	No	
Metal	Token reserve	No	Corporate	No	Yes	Fair	No	Will actively manage ex rate
Aragon	Token reserve	Yes (Estonia)	Foundation, delegated token v	Yes	Yes	Good	Yes	
Bancor	Token reserve	Yes (Zug)	Foundation based	No	Yes	Yes	Yes	Active monetary policy

Favorable jurisdictions are clearly evident from the sample, as Zug, Singapore, the Netherlands, Hong Kong, and Delaware are all popular locations to register companies and foundations.

Actual governance models are generally unspecified. Protocol level governance can often but not always be inferred from the system features, but extra-protocol governance is almost universally absent. Many projects rely on non-formalized developer consensus, and investors are satisfied to allow foundations or corporate entities control funding and hence decision-making for these nascent projects. Even when governance mechanisms (usually tokenvotes in PoS networks) are announced by developers, they often remain in limbo for months or years as other more pressing needs are prioritized, and developers focus on efficiency of feature rollout.

Finally, the inclusion in this sample of some rent-seeking shell tokens betrays the analytical poverty of the “network value” measure, or market cap as it is commonly known. Alternatively this could be classed as the hallmark of an inefficient market. While the sample was deliberately chosen to include such projects, their presence demonstrates the need for a measure of network value which captures liquidity, float, and the presence of anti-liquidity measures which drive up price. Some rankings sites include volume and trading figures from exchanges which serve only to trade one asset, and which are ripe targets for manipulation. Indeed, fabricating transaction and volume numbers on proprietary or closed exchanges is a common tactic to gain exposure, as noted in Moore and Christin (2013).

V. Unique risks for cryptoasset investors

One motivation for the cross-sectional study is to shed light on the hidden power structures behind many cryptoasset projects, which may present risks to investors. Some of these risks are exotic and novel to investors schooled in equity markets. Those profiled here include complexity risk, financing risk, and political risk.

Complexity risk

The more complex a software project, the more maintenance is required. This is found empirically in Capra, Fracalanci, and Merlo (2008). This is commonly referred to as technical

debt. Software projects are not static and require continuous updates. Adding a level of sophistication or complexity to a network increases future maintenance needs, hence the debt.

Cryptoasset markets are intensely competitive, with multiple platforms aiming to satisfy the same use-case (for instance, Maidsafe, Sia, Filecoin, and Storj all aim to provide distributed storage). They can be differentiated on complexity and ambition. Meticulously designed complex systems therefore present investor risks. This is a common argument given in favor of simple, non-Turing complete systems like Bitcoin against Turing-complete ones like Ethereum. The latter simply presents many more attack vectors, since the protocol is more permissive. Indeed, Ethereum's complexity has been the source of significant losses. The forensic investigators Chainalysis found that roughly 10% of all Ethereum earmarked for tokensales had been stolen through hacks, exploits, and phishing (Chainalysis, 2017). Exploits like the one that saw The DAO tokens siphoned from the smart contract (which had been audited) indicate the difficulty of predicting how sophisticated smart contract code will work in the wild.

Marshall (2006) adds that as complexity increases, the specialization of developers necessarily increases, and the core team becomes detached from the regular community. This leads to a breakdown of the meritocratic and open order that initially supports open source projects. Complexity may reduce the community's ability to find consensus, and drive up tensions between the rank and file and the core development team.

Financing risk

Financing risk refers to the difficulty of ensuring the conversion of contributed funds to product development. Poor conversion efficiency can result from simple expropriation, misaligned incentives, or the inability of leadership teams to allocate funds effectively. Tokenholders at present have few or no mechanisms to make ensure accountability. The "community bounty" model suffers from this, as funds are often front-loaded for the purposes of fundraising efficiency. Tokensales solve the difficulty of incentivizing contributions to an open-source network, but they introduce the risk of misspent funds. The more power a central group of developers wields over the system, and the less transparent and more complex the ownership structure, the easier it is to divert these funds. Another risk is that developers are unable to efficiently convert the growth of network value to sufficient salaries. This is common in the more voluntaristic and governance-diffuse projects. For instance, the Siacoin developers publicly considered hardforking to generate a cache of tokens for developers, as their initial allocation

was minuscule, and the fee-based model was not bringing in sufficient revenue (although they later walked back this proposal).

Political risk

The structure of the organizations and projects backing cryptoassets is no longer of academic interest. The value of the entire set of outstanding cryptoassets surpassed $100 billion in June, and over $1 billion in tokens have been issued in "Initial Coin Offerings," also referred to as Token Sales or ICOs. These are presales, usually run by corporate entities or foundations, giving investors exposure to tokens. They may be led to believe that these tokens will appreciate due to their intrinsic utility to run a protocol, due to their usage in a distributed app, because they have speculative value, or because the founders suggest that they will employ some sort of capital return mechanism to investors. These distinctions are crucially important, now that the US Securities and Exchange Commission (SEC) has taken notice of the asset class.

In a cautionary note, the SEC determined that the tokens used to crowdfund venture capital efforts on Ethereum in The DAO experiment were, in fact, securities. The SEC opted not to prosecute anyone however. The implications of the note were serious, however, as investors realized that the eye of the SEC was firmly fixed on this burgeoning market. In particular, the SEC stated clearly that "Foundational principles of the securities laws apply to virtual organizations or capital raising entities making use of distributed ledger technology," (SEC, 2017) citing the Howey test as support.

The four prongs of this test, taking to the eponymous Supreme Court decision handed down in 1946[9] bear repeating. The precise wording defines a security as "[…] an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others." It's important to note that this is a dynamic test, and that substance is privileged over style – so what investment promoters *do*, rather than *say,* is what matters. The SEC found that DAO investors invested money in a common enterprise, with the expectation of profits, and with profits deriving from the efforts of a third party – in this case, Slock.it and the curators of the contract.

[9] See SEC v. Howey Co., 328 U.S. 293 (1946)

This is crucial, as the SEC establishes that investors in a tokensale that rely on the expertise and effort of a single entity do fail that prong of the Howey test. This was undoubtedly the case for the DAO, as stated in the July report: “Through their conduct and marketing materials, Slock.it and its co-founders led investors to believe that they could be relied on to provide the significant managerial efforts required to make The DAO a success.”

Additionally, the fact that tokens held limited voting power further entrenched the status of investors as dependent upon the curators of the contract and its corporate underwriters. The SEC elaborates:

The voting rights afforded DAO Token holders did not provide them with meaningful control over the enterprise, because (1) DAO Token holders’ ability to vote for contracts was a largely perfunctory one; and (2) DAO Token holders were widely dispersed and limited in their ability to communicate with one another.

The lack of a coordinated information market to cater to DAO investors, and the general limited nature of these tokens in voting, meant that the investors did not have a legitimate ability to steer the direction of the organization.

Additionally, the utility of a token within the purported network is crucial, meaning that not all ICOs are securities. Ethereum, for instance, was launched through an ICO on the bitcoin blockchain, but was found not to be a security by the SEC, given its use as network “fuel,” in their own words. Finally, investors expecting profit is a red flag. This is broadly defined by the SEC as “dividends, other periodic payments, or the increased value of the investment.”[10]

This report focuses on US law, since the SEC is an early mover in clarifying their stance, because so many issuers are based in the US, and because its stances tend to have knock-on effects worldwide. For instance, the Monetary Authority of Singapore (MAS) subsequently released guidance (MAS, 2017) on tokensales that closely echoed the SEC’s comment.

One commonality of the prongs of the Howey test is that they mostly relate to the initial arrangement of the tokensale: crucially, whether investors expect a return, whether the tokens

[10] See SEC v. Edwards, 540 U.S. 389, 393 (2004)

have intrinsic value, and how much decision-making control issuing identities have over these collective contracts. Such a clearly defined regulatory framework makes it possible for sophisticated investors to determine, given some knowledge of cryptoasset governance, these risks. Ultimately, technological advancement is immaterial if these tokens are traded as unregistered securities and delisted from exchanges and their founders arrested. Thus a sober analysis of the corporate structure is involved is vital in defusing the uncertainty present in these markets.

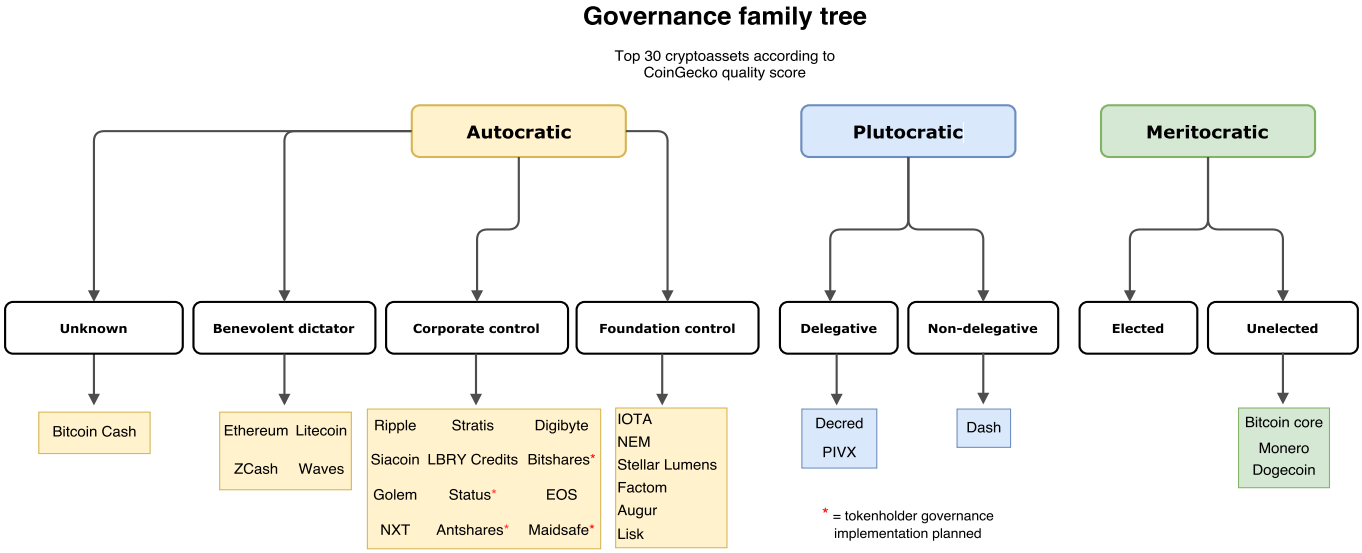
The cross-sectional industry analysis in this survey casts light on the factors linked to the risk of being regulated under securities law. In many cases, funds are centrally controlled and disbursed. Promotion and marketing is often corporate; and fundraising mechanisms are overwhelmingly ICO-driven. Eighteen of the projects surveyed promote explicit capital return mechanisms; although in staking these represent more of a redistribution of tokens from non-stakers to stakers, this is often marketed as “interest” or return. Other common mechanisms generally involve the tie-up of liquidity in exchange for some return; this is the case with masternode systems or interest payments in STEEM (with steemdollars), for instance. Other common methods include buyback programs promised to investors, financed by the success of the platform or even corporate profits; monetary policy and price floors; profit sharing from transaction fees on a subsidiary network; and profit sharing on related services.

Interestingly, many of these same projects explicitly break the linkage between the token and any promise of return, while simultaneously marketing them as sound investments. In the eyes of US regulators however, these capital return mechanisms are likely to satisfy that prong of the Howey test. Similarly, while a good number of the projects surveyed have promised to implement tokenholder governance, only a select few have delivered as promised. The constant across many of these centrally-administered projects is the promise of future shareholder-like rights – these include governance rights, voting power, and a claim to the cashflows generated by the project – yet only weak attempts to implement these. This is a manifestation of the legal grey area in which many of these projects operate. Since true collective governance methods have not yet been evidenced, many projects prefer to grant tokenholders only cursory rights and concentrate power in a central team.

VI. Cryptoasset governance explored

A table comparing the qualities of major governance models found in this survey (corporate, foundation-based, benevolent dictator, core consensus, loose consensus, masternodes, delegated staking, and Tezos-style) can be found in *Appendix A*. Drawing on the findings from the survey, *Figure 4* presents a governance family tree differentiating the broad categories in top-level governance exhibited in the sample. For the sake of simplicity, the table classifies according to the primary decision-making model exhibited. Much of the ecosystem is autocratic; and although the benevolent dictator and foundation models have precedent in FOSS projects, corporate and concentrated structures do not. Dash is non-delegative as masternode operators vote directly for proposals, mostly relating to funding.[11]

Figure 4, cryptoasset governance political classification



Context-dependent legitimacy

In times of calm, when technical roadmaps are agreed upon and incentives are aligned, governance is almost unnecessary. This is the conclusion of Gasser, Budish, and West in their 2015 study. They found legitimacy to be context dependent – so when broad approval is

[11] See Appendix B for technical detail on the Bitcoin, Dash and Decred governance models

present, light legitimacy is accepted, and when conflicts arise, a high threshold of legitimacy is required for mediation. This model explains why Ethereum progressed easily under the rule of a benevolent dictator in its early stages, yet when The DAO contract was attacked and immediate action required, leadership held a vote to find formal consensus. However, since governance methods were not operating smoothly prior to the crisis, the vote was ineffective and had low participation. This model suggests that it is worth seeking community buy-in and legitimacy even when projects are proceeding smoothly, as crises step up the demand for consensus.

Market based arbitration

When protocol decisions are fought over by intransigent parties, traditional mediation techniques fail. Occasionally, growth in a network or some exogenous shock forces leadership to confront difficult decisions. When leadership has insufficient perceived legitimacy or a sufficient level of consensus is not achieved, significant sections of the community may band together and launch a competing protocol through a hard fork.

Hard forks enact non-backwards compatible rule changes to the network. If sufficiently large groups of miners support each fork, the blockchain splits. Without proper precautions, they can cause substantial confusion, token losses, and misspent transactions. Two notable examples are worth discussing: one in which the amended protocol gained wider adoption, and one in which the original protocol retained the majority of the economic activity and value.

The hard fork outcome matrix below (*Figure 5*) defines the possible outcomes of a contested hard fork. This models the ways in which the market determines existential outcomes. Whichever chain reaches widespread adoption, network value, economic activity, and mainstream legitimacy, obtains or retains the perception as the true asset.

Hard fork outcome matrix

Where O is original protocol and A is the amended protocol

	Market supports A	**Market rejects A**
Market supports O	Network value split in some combination of O and A	Original protocol predominates
Market rejects O	Amended protocol predominates	Protocol abandoned due to loss of trust

Figure 5, market-based arbitration methods

Since copyrights are irrelevant to an open source network, and legitimacy is a function of perception rather than corporate structure, among politically decentralized protocols, the market is called upon to determine which protocol can lay claim to the name.

In 2015, when founders of Ethereum network, together with a startup Slock.it, launched The DAO, promotional materials promised unstoppable, distributed contracts, and 'code is law' governance (Dahub, 2016). When a smart contract in The DAO was exploited and roughly $50 million in ether was drained from the fund, the community faced a stark choice: rewrite the history of the blockchain, violating the promises made in promotional materials, or swallow the loss.

Ethereum leadership, including creator Vitalik Buterin, advocated for the first option, and helped orchestrate a hard fork to recoup the losses (documented in Atzei, Bartoletti, Cimoli 2017). They held a hurried vote, although this failed to generate more than a single digit quorum. Some DAO tokenholders and Ethereum community members rejected the amendment to the protocol, believing that it would compromise immutability and Ethereum's stated values. Thus the original chain was unexpectedly supported with miner hashpower and eventually, economic and developer activity. The protest chain was dubbed Ethereum Classic. Today, the two chains coexist, although Ethereum (the amended protocol) dominates in node count, users, network value, and developer activity. In this instance, the vote to achieve community consensus was ineffectual, and so the mediation of the dispute was put to the market through the hard fork mechanism. Due to support from the Ethereum founder and benevolent dictator Vitalik Buterin, the amended chain won the lion's share. Despite this, Ethereum Classic persists. Thus while

there was a clear winner according to the market, the Ethereum split belongs in the upper left quadrant of the hard fork matrix, as an equilibrium between the contested chains was found.

Another notable hard fork occurred in August 2017, when a competing faction of miners and advocates created a hard fork on the Bitcoin protocol. This was precipitated by the adoption of the SegWit upgrade to the protocol. SegWit is an improvement which sets the stage for Bitcoin becoming a two-layer network, with settlement on the base layer and transactions on the top layer. This vision was incompatible with that of some advocates, who wanted to scale the network by increasing the size of 10-minute blocks, rather than building another network on top. In response to the SegWit activation, and perceived censorship and a lack of cooperation on the part of the core developers, a group of miners and developers, led by the Chinese exchange ViaBTC, launched Bitcoin Cash, an incompatible hard fork of the Bitcoin protocol. Everyone owning Bitcoin on August 1st came to own an equivalent amount of Bitcoin Cash. The market was left to decide. Although it is too early to tell, current exchange rates see Bitcoin Cash trading at roughly 7% of the value of original Bitcoin. Thus early indications suggest that the incumbent survived unaffected. Despite this, Bitcoin Cash has a network value in excess of $5 billion dollars at the time of writing, indicating conditional success. Currently this development occupies the top left hand corner of the hard fork matrix, although Bitcoin's dominance is largely unperturbed by the hard fork.

These two examples with radically different outcomes illustrate the danger that a hard fork poses to the incumbent protocol. However in both cases, the 'winning' chain was that which was supported by the chief actors – in Ethereum's case, the foundation and Vitalik Buterin supported the forked chain, and in Bitcoin's the core developers supported the original chain.

Custodial products and the importance of formalized governance

The prevalence of hard forks as a dispute-resolution mechanism has troubling implications for custodial services. Imagine an ETF issuer offering investors exposure to Bitcoin, which undergoes a hard fork. The provider is now in the difficult position of selecting the "true" chain. This is more than just an academic exercise, as the Grayscale Bitcoin Investment Trust recently had to select Bitcoin Core as the appropriate chain and agreed to sell off the duplicated and modified Bitcoin Cash chain. In this case, it was a fairly trivial exercise, as Bitcoin Cash was the clear minority fork, but one can easily imagine a 50/50 split where the dominant chain isn't clear for some time.

In a politically decentralized system, such as Bitcoin, no one has the authority to decide which chain is the original. Solutions such as "the longest valid chain" work in weakly contested forks, but provide little help in cases of sincere disagreements. In this case, the actions of large custodians may actually inform the ultimate winner, as they control significant fractions of the market, and can choose to sell their duplicated forked tokens and crash one chain or the other. The use of hard fork arbitration is therefore elegant from the perspective of the efficient markets believer, yet troubling for custodians and their clients. They may welcome the rise of a staked token which has transparent, widely used on-chain voting mechanisms, which can provide a formal bellwether of which fork the community agrees with – or which could allay tensions in the first place, reducing the risk of a contested hard fork. Additionally, the benevolent dictator can provide clarity in resolving "ship of Theseus"[12] problems by dubbing one chain in a fork the true chain, as Buterin did with Ethereum. However since Buterin was a large stakeholder in Ethereum at the time of the fork, and affiliated Ethereum Foundation accounts held provably large sums of DAO tokens, the independence of leadership can be questioned here.

Incentive alignment and agency problems

Cryptoasset ownership is often heavily concentrated, untransparent, and in many cases anonymous by design. Kondor et al find that in May 2013, Bitcoin's Gini coefficient was a highly unequal 0.985 (2014). The inherent desire for privacy and non-public ownership details render coordination among investors difficult. The rise of custodians such as the Greyscale Bitcoin Trust, Coinbase, and the numerous hedge funds entering the space might enhance coordination. Indeed, Barry Silbert, the owner of Digital Currency Group (DCG), is credited with making the compromise that saw miners and developers provisionally unite over a Bitcoin scaling solution in May 2017 (DCG, 2017).

Agency problems are severe in a fragmented system. As Brudney (1985) notes, "scattered shareholders lack the requisite information and institutional mechanisms either to bargain over the terms of management's employment, or to monitor and control management's activities." This problem, already distinct in equity markets, is considerably exacerbated in cryptoasset

[12] The Ship of Theseus is a thought experiment in which parts of the ship are gradually replaced, until none of the original ship remains. Those parts are used to construct another ship. Which is the original? The paradox illustrates the difficult in assigning identity in a mutable system. Nonproprietary open-source projects with no single leader are vulnerable to issues of identity permanence.

markets. Information markets are poor, almost no mechanisms exist to make developers and founders accountable, “firing” developers in an open-source and voluntarist network is almost impossible, and tokenholders are generally disempowered. For the activist investor, cryptoassets are starkly lacking in power structures that privilege investors over founders or developers.

Of the top fifty assets by network value, only nine had explicitly defined governance structures, with nine more having partially defined them or having committed to iterating them at a future date. Additionally, most of these refer to protocol governance, rather than granting stakeholders extra-protocol powers over developers, founders, foundations, or CEOs. Some foundations exist to passively coordinate the flow of contributed funds to developers and to facilitate open-source development and employment within a jurisdictional environment; others however concentrate power, control development roadmaps, hire developers exclusively, and maintain sole control over funding. Corporate projects are invariably more concentrated in power, and even sometimes depart from the open-source model that gave rise to the ecosystem. While the foundation model has been pioneered for long-running, successful open source projects like Linux or Apache, it original purpose – to unintrusively foster the growth of an independent, voluntarist network – has been left behind in many projects. Many foundations serve as a rubber stamp for founder decision-making and to shield them from regulators.

The projects that grant tokenholders rights are those with some Proof of Stake component; in Proof of Work systems, power is concentrated instead among miners, economic nodes operators, and developers. It’s nontrivial to amass a “voting” quantity of hash power in a PoW network. It requires significant technical expertise, economic investment, and a favorable geographic location (with cheap electricity and cooling and good internet). Often, ASICs are sold by few or a single supplier, who may be leery of selling them to a competitor, granting them monopolistic control over the market. Thus the measurable work that goes into a PoW currency constricts the ability of would-be activist investors to influence it on the protocol level. Proof of Work advocates maintain this as a relative strength, as ASICs align miners’ long-term incentives with the success of the protocol, and this insulates the currency from speculative attacks as hashpower is difficult to accumulate. However from a governance perspective this means that tokenholders are dis-empowered in PoW networks.

PoS networks are therefore the main source of tokenholder rights. These explicitly privilege large blockholders, by granting them a preferential claim on the proceeds from continuous dilution or transaction fees. As Van Valkenburgh notes, PoS systems are inherently centralizative, and their natural conclusion if not impeded is the domination of the system by a central agent or cabal (2016). This does however make them good candidates for investors. Dash for instance grants masternode operators a vote over how to spend the percentage of each block reward which is held in reserve for community funding.

Indeed, anonymity, collective-action problems, and technical impediments to voting significantly impeded consensus-finding in the weeks after the hack of The DAO. The Ethereum leadership hosted a vote to determine whether to hard fork or not which was explicitly branded as the ultimate decider: “At block number 1894000 the votes will be tallied, and the outcome will determine whether the default is set ***to fork*** or ***not to fork”*** (Wilke, 2016). However, only 8.3% of all outstanding ether tokens participated in the vote, with 20.98% of the total votes coming from a single address. This vote was taken as community assent, with predictably disastrous results. A portion of the Ethereum community grew permanently disaffected with the leadership and the violation of the immutability promise, remaining on the legacy chain, even though that exposed them to the loss of tokens stolen from The DAO.

Principal-agent problems are a useful conceptual lens through which to analyze network structures. Since many of these experiments involve novel firm designs, in which traditional corporate structures are replaced by a confederation of stakeholders, these concerns are acutely relevant. As Jensen and Meckling note in their seminal paper, “agency costs arise in any situation involving cooperative effort […] by two or more people even though there is no clear cut principal-agent relationship” (1976). Programming is a largely individual effort, and so networks representing billions in value may depend on the work done by a handful of individuals. Agency problems are exacerbated by the technical chasm between developers working on obscure cryptographic protocols and investor expertise. In systems where tokenholders own the system, they still face frictions to exerting authority over it. Collective action difficulties, heterogeneous investor goals, and weak transparency complicate coordination.

Incentive alignment in developer funding models

Jensen and Meckling find in their paper on agency costs that as the owner's fraction of equity falls, his incentive to expropriate wealth from the company increases. This appears to run contrary to conventional wisdom in cryptoasset investing, where founders owning a large percentage of outstanding tokens is commonly held as a risk factor, as Van Valkenburgh (2016) cautions. However, these are not necessarily in conflict. Overly premined coins (or those where founders keep a large percentage in reserve) are often treated with suspicion as they are costless to create. However most communities tolerate some token reserve to fund ongoing development. Hence an equilibrium is found between the level of dilution investors will tolerate, and between the requirements of developers to bootstrap a successful project. In the 50 projects surveyed, the mean token reserve for founders and developers was 19.68 percent of the total supply. While significant founder holdings do closely align incentives with those of tokenholders, exceeding some acceptable threshold is punished by the market. In staked or masternode systems, high founder allocations grant them near-total power over the direction of the protect.

However, much as the corporate governance literature notes the perverse incentives that come from granting CEOs stock options with high convexity, founders wishing to extract rent from their cryptoassets may try to artificially inflate prices by introducing liquidity lock-up measures for users (hence the common anti-liquidity measures evidenced in tokens like STEEM) and by manipulating market sentiment with optimistic announcements. Since investor protection measures like vesting periods, blackout periods, and insider trading regulation are completely absent from the space, founder reserves are suboptimal.

In a currency or protocol networks, a measure of success is not just the total outstanding value of the network (as it would be trivial to create a trillion-dollar cryptocurrency by "minting" one trillion and selling one for a dollar) but rather the actual acceptance and circulation of the tokens. Thus founders receiving payment on a transactional as well as value basis would be better incentivized to promote the health of the network with regards to its metrics of actual usage. The Siacoin model, whereby a portion of each contract for distribute cloud storage is paid as a fee to developers, is a good example. Additionally, payment structures that fund developers over time, rather than in a huge initial distribution, mollify these perverse incentives. Zcash, Dash, and Decred pay founders directly or indirectly by allocating them a portion of the block reward. This incentivizes them to remain with the project, as they are paid on a continuous basis. The

crowdfunded community bounty model directly links community demand for features and software development with their funding. However, this falls prey to free rider difficulties and collective action problems. Some projects have corporate sponsors who effectively subsidize the public good by paying a few full-time developers, as is the case with Bitcoin. This however leads to legitimacy problems as the community may suspect a perversion of developer motives, especially if those companies extract rent from the platform in some way. There is clearly no best model for funding developers; they represent a set of tradeoffs between healthy developer funding, perceived legitimacy, long-term incentive alignment, and efficiency.

Conclusion

The principal contribution of this study is to expose the curious disjunction between the public pronouncements of tokensale promoters – that tokens represent a claim on the value of the network – and the legal disclosures they make investors sign, which state that the tokens are valueless.

Developers and promoters market the assets as security-like, vaguely (or explicitly) promising capital return mechanisms, while simultaneously denying that the tokens sold have any value or governance rights whatsoever. ICO promotion is a game of brinksmanship between convincing investors that the tokens sold will endow them with rights to use and profit from the network, and convincing regulators that the tokens do not represent securities. It may ultimately prove to be an impossible balancing act.

Regulators and investors may expect developers to self-police and willingly surrender power, after initially consolidating it in a token sale. Many projects promise to introduce some level of decentralization at the governance level, to accompany the protocol-level decentralization. However, most projects grant tokenholders only specious governance power. Unlike equity shareholders, token-holders cannot vote to oust the founders from the project. Typical votes concern cosmetic or trivial issues, and are often met by apathy. Relatively few serious, existential disputes have been mediated by a formal tokenvote. In those extreme situations, market-based hard fork economics are preferred.

Poor political decentralization is not necessarily due to maliciousness on the part of the organizers, as startups and emerging projects require initial centralization. But promising

decentralization and failing to deliver not only represents a broken promise to investors, but raises risks of expropriation and exposes founders to the risk of being branded sellers of unlicensed securities. Yarvin labels this “decentralization theater” (2016).

There is a delicate tradeoff involved in designing a ‘decentralized’ system: for the protocol to be created, a first mover is necessary. By definition, the creator has initial control over the attributes of the system. So a decentralized system can never, at inception, be decentralized on a governance level, unless the founder willingly renounces control – like Satoshi Nakamoto did in 2011. The practical realities of controlling fundraising, intellectual property, and hiring in a given jurisdiction also require some degree of centralization. Firms exist to take advantage of economies of scale, and recognize the efficiencies inherent in hierarchical structure. Adapting the startup and fundraising model to the decentralized, open source model has therefore proved extremely difficult. The centralization of power and control is not inherently wrong – it’s the ideological foundation of the modern state and corporate system – but it does result in paradoxes when applied to decentralized networks.

The incredible success of the Bitcoin protocol demonstrated, for the first time, the success of a free open source network in which the protocol itself was monetized. Other successful FOSS networks like Linux, Apache, and Netbeans were not financially impregnated at the system level, and thus escaped the perverse (and rent-seeking) incentives that accompany a moneyed system. In the case of Bitcoin, the necessary computational work required to obtain tokens gave it a “fair” launch and ensured that it could not be individually controlled. Satoshi’s resignation from the project, and its ultimate meritocratic and open governance structure granted it additional credibility. Finally, its carefully poised miner - developer - node governance structure ensured that protocol upgrades required overwhelming community consensus. Bitcoin is a pioneering and successful model of open, community-led, meritocratic governance, but the model has only seen sparse adoption.

A great number of paradoxes plague the emergent asset class. Incentives are aligned when developers control some percentage of tokens, yet they should be wary of overly-large developer allocations. Tokensale promoters advertise capital return mechanisms and governance rights, yet explicitly disavow these token functions in legal disclosures. Centrally-administered projects are often the most efficient, yet maintain the least community legitimacy. Open-source networks are a rebellion against corporate interests, yet most projects are

corporate-administered. Investors may think seeking out projects which are efficiently operated, grant them voting rights, and a claim on the protocol's cash flows is a way to select sound investments; yet these are the features of projects which are most likely to see them branded as unregistered securities. Incentives must be aligned and developers need financing, yet these financing methods grant developers unlimited power and risk expropriation of investor funds. And governance failures and impasses, like the problems currently plaguing Bitcoin, may actually be evidence of a thriving, well-poised power structure.

Some best practices can be found: founders are expected to self-police, so transparency is required. Decentralized funding models are possible and encouraged. Large or obscure premines and token reserves are discouraged. A 'block reward' development fee model better aligns developer incentives with continuing project success. Tokenvotes should grant investors more than cursory powers over the project, if implemented. Finally, developers should determine whether their token is a utility token, an investment token, or something else – and align their disclosures with actual token usage. Investors should be wary of shell tokens and exercise their governance rights when granted them.

The sober conclusion from this survey of the largest projects by market perception is that investors are largely unconcerned with obtaining governance rights, and where they do possess them, they do not use them efficiently. Today, most projects are characterized by the concentration of power in the hands of a few individuals. The entry into the space of traditional investors may cause a shift towards explicit shareholder rights, and this is evidenced in the emergence of projects like Dash, Decred, and Tezos. Yet projects which grant tokenholders or node-operators voting rights are beset by issues of power concentration. Finding a fair distribution method is therefore required. However, no such method has been evidenced, beyond mining and airdrops, and no good compromise has been found between efficiency and community buy-in thus far. It remains to be seen whether decentralized governance is a legitimate proposition or a pipe dream.

References:

Ansell, Chris, and Alison Gash. "Collaborative governance in theory and practice." *Journal of public administration research and theory* 18.4 (2008): 543-571.

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. "A Survey of Attacks on Ethereum Smart Contracts (SoK)." *International Conference on Principles of Security and Trust*. Springer, Berlin, Heidelberg, 2017.

Bentov, Iddo, Lee, C., Mizrahi, A., and Rosenfeld, M. "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake." *ACM SIGMETRICS Performance Evaluation Review* 42.3 (2014): 34-37.

Bitcoincash.org. "Frequently asked questions." *Bitcoincash.org.* (2017). Retrieved from https://www.bitcoincash.org/.

Bitcointalk.org anonymous poster. "Blowing the lid off the CryptoNote/Bytecoin scam" *Bitcointalk.org.* Aug. 2014. Retrieved from https://bitcointalk.org/index.php?topic=740112.0.

Blanch, Francisco. "Bitcoin: a New Liquid Market?" *Bank of America Merrill Lynch research* (2017)

Bonneau, Joseph et al. "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" *IEEE Security and Privacy* (2015): 1-19.

Brito, Jerry, and Andrea Castillo. *Bitcoin: A primer for policymakers*. Mercatus Center at George Mason University, 2013. 1-43

Brudney, Victor. "Corporate governance, agency costs, and the rhetoric of contract." *Columbia Law Review* (1985): 1403-1444.

Burniske, Chris, and Jack Tatar. *Cryptoassets The Innovative Investor's Guide to Bitcoin and Beyond*. McGraw-Hill, 2017.

Burniske, Chris., and A. White. "Bitcoin: ringing the bell for a new asset class." *Ark Invest and Coinbase* (2016).

Capra, Eugenio, Chiara Francalanci, and Francesco Merlo. "An empirical study on the relationship between software design quality, development effort and governance in open source projects." *IEEE Transactions on Software Engineering* 34.6 (2008): 765-782.

Chainalysis. "The Rise of Cybercrime on Ethereum," *Chainalysis blog.* Aug. 07, 2017. Retrieved from https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/.

Cisco. "Cisco Visual Networking Index: Forecast and Methodology, 2016–2021." *Cisco public white paper.* 2016, updated 2017. Retrived from https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

Coglianese, Cary. "Assessing Consensus: The Promise and Performance of Negotiated Rulemaking." *Duke Law Journal*, vol. 46, no. 6, 1997, p. 1255., doi:10.2307/1372989.

Daohub. "Explanation of Terms and Disclaimer," *Daohub.org.* Apr. 2016. Archived at https://web.archive.org/web/20160501124801/https://daohub.org/explainer.html.

De Filippi, Primavera, and Benjamin Loveluck. 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure*." Internet Policy Review* 5 (3). https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governancecrisis-decentralised-infrastructure.

De Laat, Paul B. "Governance of open source software: state of the art." *Journal of Management & Governance* 11.2 (2007): 165-177.

Digital Currency Group. "Bitcoin Scaling Agreement at Consensus 2017" *DCG on Medium.org.* May 23, 2017. Retrieved from https://medium.com/@DCGco/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77.

Elendner, Hermann, et al. *The cross-section of crypto-currencies as financial assets: An overview*. No. 2016-038. SFB 649 Discussion Paper, 2016.

FinCEN. "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." *FinCEN.gov*, Department of the Treasury Financial Crimes Enforcement Network, 18 Mar. 2013. Retrieved from www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

Franck, Egon, and Carola Jungwirth. "Reconciling rent-seekers and donators–The governance structure of open source." *Journal of Management and Governance* 7.4 (2003): 401-421.

Gall, John. *Systemantics: how systems work and especially how they fail*. Times Books, 1977.

Garcia, David, et al. "The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy." *Journal of the Royal Society Interface* 11.99 (2014): 20140623.
Gasser, U., Budish, R., West, S. M., "Multistakeholder as Governance Groups: Observations from Case Studies." *Berkman Center Research Publication* 1 (2015). Retrieved from http://ssrn.com/abstract=2549270
Gervais, Arthur, et al. "Is Bitcoin a decentralized currency?." *IEEE security & privacy* 12.3 (2014): 54-60.
http://www.truthcoin.info/blog/measuring-decentralization/
IRS. "IRS Virtual Currency Guidance" *Internal Revenue Service Bulletin,* April 14, 2014. Retrieved from https://www.irs.gov/irb/2014-16_IRB/ar12.html
Jensen, Chris, and Walt Scacchi. "Governance in open source software development projects: A comparative multi-level analysis." *Open Source Software: New Horizons* (2010): 130-142.
Jensen, Michael C., and William H. Meckling. "Theory of the firm: Managerial behavior, agency costs and ownership structure." *Journal of financial economics* 3.4 (1976): 305-360.
King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." *self-published paper, August* 19 (2012). Retrieved from http://peerco.in/assets/paper/peercoin-paper.pdf
Lamport, Leslie, Robert Shostak, and Marshall Pease. "The Byzantine generals problem." *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4.3 (1982): 382-401.
Lerner, Josh, and Jean Tirole. "Some simple economics of open source." *The journal of industrial economics* 50.2 (2002): 197-234.
Marshall, Jonathan. "Negri, Hardt, distributed governance and open source software." *PORTAL Journal of Multidisciplinary International Studies* 3.1 (2006).
Monetary Authority of Singapore. "MAS clarifies regulatory position on the offer of digital tokens in Singapore," *MAS.gov Press Release*s. Aug. 1, 2017. Retrieved from http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx.
Moore, Tyler, and Nicolas Christin. "Beware the middleman: Empirical analysis of Bitcoin-exchange risk." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2013.
Nakamoto, Satoshi. "Bitcoin open source implementation of P2P currency." *P2P Foundation* 18 (2009).
Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.
Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies v1", *Coin Center Report* (2016). Retrieved from https://coincenter.org/2016/01/securities-framework/
Popper, Nathaniel, and Ruiz, Rebecca. "2 Leading Online Black Markets Are Shut Down by Authorities" *New York Times.* (2017). Retrieved from https://www.nytimes.com/2017/07/20/business/dealbook/alphabay-dark-web-opioids.html?mcubz=1
Popper, Nathaniel. "Bitcoin Exchange Was a Nexus of Crime, Indictment Says," *New York Times.* (2017). Retrieved from https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html?mcubz=1
Popper, Nathaniel. *Digital Gold: the Untold Story of Bitcoin*. Penguin Books, 2015.
Raymond, Eric Steven. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O'Reilly, 2009.
Reijers, Wessel, Fiachra O'Brolcháin, and Paul Haynes. "Governance in Blockchain Technologies & Social Contract Theories." *Ledger* 1 (2016): 134-151.
Schneider, Aaron. "Decentralization: Conceptualization and measurement." *Studies in comparative international development* 38.3 (2003): 32.
Securities and Exchange Commission. "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO," *SEC.gov.* July 25, 2017. Retrieved from https://www.sec.gov/litigation/investreport/34-81207.pdf
Srinivasan, Balaji, and Lee, Leland. "Quantifying Decentralization." *21.co*. July 27, 2017. Retrieved from https://news.21.co/quantifying-decentralization-e39db233c28e
Sztorc, Paul (a). "Nothing Is Cheaper than Proof of Work." *Truthcoin*, Aug. 4 2015, Retrieved from www.truthcoin.info/blog/pow-cheapest/.
Sztorc, Paul (b). "Measuring Decentralization." *Truthcoin,* Sep. 9, 2015. Retrieved from
Wilke, Jeffrey. "To fork or not to fork," *Ethereum.org*. July 15, 2016. Retrieved from https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/

Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum Project Yellow Paper* 151 (2014).
Yarvin, Curtis. “The DAO as a lesson in decentralized governance” *Urbit.org*. Accessed 24 June 2016, urbit.org/blog/dao/.
Yermack, David. "Corporate governance and blockchains." *Review of Finance* 21.1 (2017): 7-31.

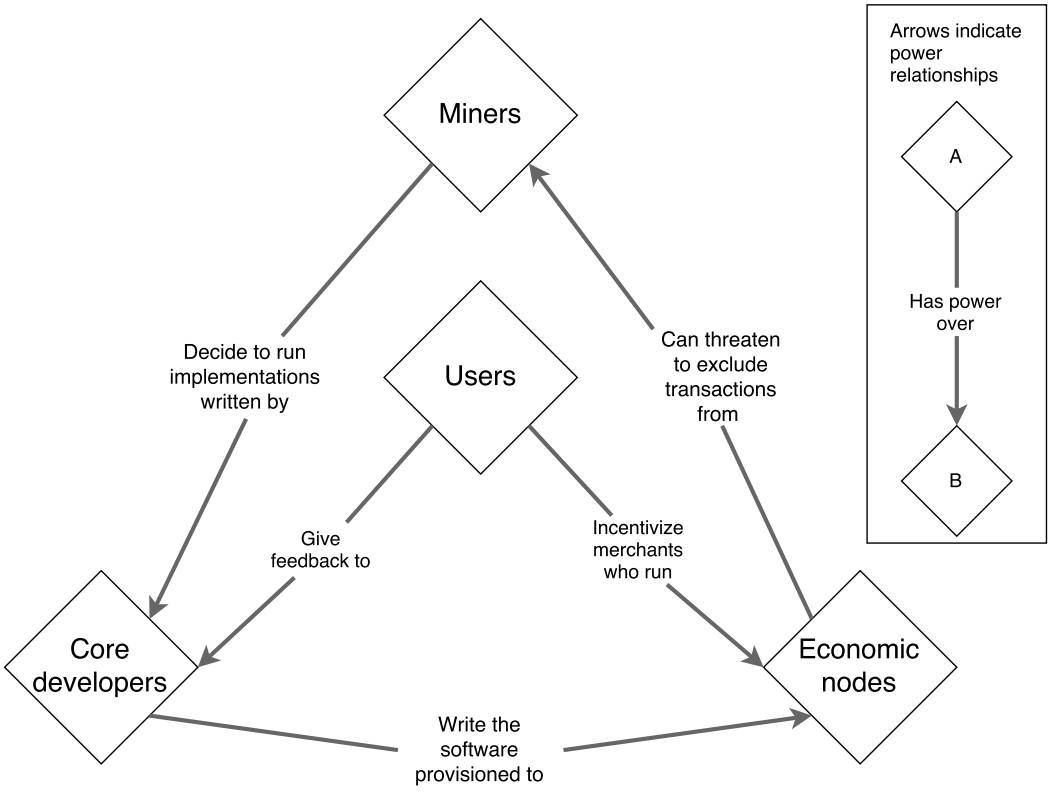
Appendices

Appendix A:
Common traits of major governance models covered in the survey

	Corporate	Foundation	Benevolent dictator	Core consensus	Loose consensus	Masternodes	Delegated staking	Tezos-style
On chain governance	None	None	None	Miner-node-interplay	Miner-node-interplay	Possible, limited	Possible	Possible
Off chain governance	Corporate	Foundation	Consultation-style	Community discussion	Developer discussion	Unlikely	Possible, assembly style	Designed for
Decision-making transparency	Variable	Variable	Fair to good	Good to fair	Good to fair	Fair	Good	Excellent
Political risk	High	Depends on foundation use	Medium	Low	Very low	Moderate	Low	Low
Governance decentralization	Poor	Poor	Poor	Fair	Fair to good	Depends on dispersion	Depends on dispersion	Good
Efficiency	Excellent	Good	Excellent	Good	Fair	Fair	Fair	Poor
Principal funding model	Corporate income	Token reserve/donor	Multiple	Voluntarism, bounties	Voluntarism, bounties	Bounties, dev. pools	Dev. pools, token reserve	Token reserve
Voting domain	n/a	n/a	n/a	n/a	n/a	Funding	Funding, assemblies, limited	Entire protocol
Miner control (in PoW)	Minimal	Variable	Significant	Significant	Significant	Overridden	Overridden	n/a
'Ship of Theseus' problems	Nonexistent	Almost nonexistent	Defused	Common	Common	Unlikely	Unlikely	Unlikely
Anonymous decisionmakers	Almost impossible	Rare/difficult	Possible	Fairly common	Common	Common	Less common	Common
Importance of reputation	Less important	Less important	Important	Important	Somewhat important	Less important	Important	Less important
Governance requires capital lockup	No	Not required, but common	No	No	No	Yes, but can be withdrawn	Yes, hard to withdraw	No
Community support	Not required	Variable	Not required, but useful	Required	Required	Useful	Required	Required
Proprietary development	Common	Common	Rare	Absent	Absent	Rare	Rare	n/a
Required community consensus	None	Little	Moderate	High	Extreme	Moderate/variable	High	High
Dispute resolution mechanism	Hierarchical	Unspecified/hierarchical	Consultation-style	Public discussion	Public discussion	Voting	Voting	Voting
Governance scalability	High	High	Good	Moderate	Fair	Fair	Fair	Poor
Ability for large token holder to coopt	Nonexistent	Low	Nonexistent	Medium	Low	High	High	High
Potential flow of wealth redistribution	Investors to founders	Investors to entrepreneurs	Investors to B.D. & associates	Investors to miners	Investors to miners	Investors to node operators	Small stakers to large stakers	n/a

Appendix B:
Technical detail on the Bitcoin, Dash, and Decred governance models

Bitcoin's governance is set out in De Philippi and Loveluck (2016) as an intensely technocratic and closed process among core developers. However recent events challenge this model. Alternative implementations, starting with Bitcoin Cash, were released, invoking market-based arbitration. Prior to this, miners held provably large power relative to developers by blocking the SegWit implementation. This 'veto' was subsequently overruled by the community in the form of the User Activated Soft Fork rebellion, which escalated the debate and saw miners implement SegWit. Protocol-level actions by miners affect extra-protocol decisions by developers, although not exclusively. Thus a tripartite model is set out here, detailed in the figure below.



Dash ("digital cash") is a cryptocurrency aiming to facilitate rapid transactions and optional private transactions. It exhibits a two-tier node structure consisting of masternodes and regular nodes. Masternodes are non-mining nodes which receive 45% of block rewards (with 45% going to miners and 10% to a pooled development fund) in exchange for performing governance functions and enabling the *PrivateSend* and *InstantSend* transactions. They can be purchased by locking up 1000 Dash as collateral (equivalent to $295,000 at the time of writing) to incentivize network support. Masternode owners are the owners of the network, as they vote on protocol decisions and over the use of development funds. Developers however remain the ultimate arbiters of what is implemented, and masternode owners have no demonstrated ability to enforce their position in the case of a disagreement.

By implementing a threshold-based franchise, the Dash network not only grants more voting power to wealthy tokenholders, but entirely excludes the vast majority of participants. The unequal initial distribution heightens these disparities and concentrates power in the hands of a

few. Finally, as far as governance rights are concerned, the votes are often treated as suggestions rather than mandates by the core team. Sammons (2016) investigates 180 proposals and finds masternode owners lacking in the ability to enforce accountability on funded projects, and finds a heavy concentration in submitters; at the time, 88% of funds allocated came from proposals submitted by only two individuals.

Decred ("decentralized credit") is a cryptocurrency aimed at solving problems of governance found with Bitcoin. It has specifically defined on and off-chain governance mechanisms. To avoid Theseus difficulties, Decred has a constitution dictating protocol and extra-protocol governance, and temporary custodians in Decred Holdings Group LLC. A hybrid Proof of Work/ Proof of Stake system grants tokenholders a veto over miners if 60% of stakers agree. Voting is probabilistic and requires the lockup of funds until a vote occurs, with typical wait times averaging 28 days. Barriers to entry are low; in recent months entering a voting ticket requires approximately 50 DCR, or $1250 at current exchange rates. Governance decisions are made by the Decred Assembly, an elected body. Decred's lower barrier to entry is more participative than Dash, and governance deliberations are formalized. However development currently takes place under the aegis of a corporation, and on-chain governance is still limited. Funding is sustainably determined by a block subsidy. Project governance is excessively complex and formal deliberation in this domain appears largely inactive at present.