Academic

Nelson Bighetti

Search

Academic

- Home
- Posts
- Projects
- Publications
- Contact
-
-

Introduction

DRAFT: This has not yet been released so please do not share it yet.

Introduction

This resource presents a view of blockchains and cryptocurrencies as common pool resources, and as products of commons-based peer production. These concepts will be introduced, and their relevance to understanding blockchains ecosystems will be explored. I will present a view of cryptocurrencies as significant new forms of commons-based peer production, that have in some cases managed to overcome the incentives/funding issue which often limits the scale of FOSS volunteer collectives and what they can produce.

Bitcoin is a resilient social organism, native to the free digital commons. Participation in the Bitcoin network is open to all, the distributed ledger and software to read and interact with it are freely available and open source. The network is peer to peer, which gives it the same decentralized redundancy and resilience to shutdown as the Bittorrent protocol. For as long as people want to participate

in Bitcoin and have the means to communicate, it is safe to assume that the network will be operating in at least some capacity. Given that the network is here to stay, and the people who embrace it have grand ambitions for its societal impact, it is important to understand the social and relational dynamics at play among participants, as these will determine how the network behaves in the long run.

The network is actively constructed by its human participants, who can be considered as a set of constituencies that each do their part to give value to the network and its native assets. There are two key constituencies driving the network: the developers of the blockchain's software infrastructure, and the producers of blocks on the network (miners). I consider how those constituencies interact with each other, and the other constituencies that contribute to giving the network value (merchants, service providers, node operators, users).

The work of Elinor Ostrom will be used to consider the resources these networks produce as **common pool resources**. Blockchains are in a sense public goods, because they are accessible to all, but the resource they produce (incorruptible public ledger open to all, providing the capacity to make uncensorable transactions) is necessarily finite (because scale comes at a cost to nodes in the network).

The work of Yochai Benkler will be used to consider the production of these resources as a form of **commons-based peer production**, and the software they run on will be considered as examples of Free Libre Open Source Software (FLOSS). My position is that blockchain projects are significant as new forms of commons-based peer production which incentivize the production effort much more effectively than prior forms. Blockchains, therefore, have the potential to harness the power of commons-based peer production at greater scale and be of greater consequence to wider society.

The blockchain itself is a new form of digital commons where the rules are enforced collectively by all participants. We are witnessing a flurry of experimentation in how the novel affordances of this decentralized commons can be used to facilitate new modes of organization and coordination.

The first part of this resource introduces the concepts and considers what is familiar and what is different about the cryptocurrency context. A framework is developed which involves profiling the constituencies that make up a blockchain's ecosystem and considering the roles they play and how they interact with each other.

In part 2 of the resource, this framework is then applied to characterize a number of projects based on observations of their commons. This is composed of a set of reviews of blockchain-type projects from the perspective of common pool resources and commons-based peer production.

Decentralized Autonomous Organizations (DAOs) have emerged as an effort to harness the coordination and organizational affordances of blockchains. I will

consider some examples of DAOs that are being used as part of the governance of cryptocurrency networks, and also some platforms which exist to allow for the creation of DAOs with varied purposes.

This is version 0.5.0 - I consider this a not quite public beta, the purpose of which is to collect feedback which can be used to improve the resource before launching it properly.

I am planning to develop this resource on an ongoing basis, and will collect updates into releases with release notes that explain what has changed - you can follow the full history of how it develops in the GitHub repository, and check the diff to see what has changed since the last version you read.

This resource is closely related to the crypto governance research repository, which collects answers to a standardized set of questions for a variety of projects. That repository is open for contributions. A good reason to try and open this up is that there is simply too much going on in the space for one or a small number of contributors to track.

Commons Based Peer Production (CBPP)

Yochai Benkler (2006) wrote about the concept of commons-based peer production in his 2006 book "The Wealth of Networks - How Social Production Transforms Markets and Freedom", describing its qualities and potential in some detail. Commons based peer production (CBPP) is a new model of socioeconomic production in which people work cooperatively on commons-based (publicly accessible) resources. The most well described and significant examples of CBPP are Free and Open Source Software (FOSS) projects, other examples include Wikipedia, OpenStreetMap and The Pirate Bay.

The Internet has dramatically lowered communications costs, and the costs associated with providing information goods. These developments made CBPP possible because they allowed people who shared a common interest to find each other, communicate, share work on a common project, and distribute the product of that work to anyone who wanted it. The low costs associated with communication, production, and distribution meant that there was no need for an organization with capital to take ownership of the projects and run them in a way which would generate revenue.

With these barriers removed, groups of hobbyists could collaborate on projects that they found interesting or useful - and this mode of production has given us the software that the bulk of the Internet runs on. Nadia Eghbal's Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure provides an excellent account of the importance of FOSS to our digital infrastructure, why there are issues with funding it and what the consequences are.

The way in which participants collaborate, and the nature of the resource they produce, are also fundamental to CBPP. This mode of production is characterized

by openness. In the case of FOSS the software is open-source, so anyone can read the code, understand it, and tweak or re-purpose it. This widens the pool of potential contributors to include anyone with an interest in the project who takes the time to understand the product and how it is being produced.

Licensing also plays a role here, with the advent of "copyleft" licenses like the GNU General Public License allowing groups to protect their work and guarantee that they could continue to use and build on the resource, while also preventing any actor from making a proprietary restricted-access version of that resource.

Unrestricted access to the resource and its history results in a kind of equality between participants (peers). Should a conflict arise about the project's direction the conflicting parties have an option to "fork" the resource and develop alternative versions from that point onwards.

CBPP projects typically lack a hierarchical or otherwise tightly defined structure, peers participate independently on a voluntary basis, assigning themselves to the tasks they find most interesting or worthwhile. This method of open voluntary allocation seems to offer high efficiency in allocating human resources - more so than top-down management within conventional organizations (with Human Resources departments). GitHub, a key platform for the software commons, and itself valued in the billions of dollars when acquired by Microsoft, relies on open allocation internally. Spotify also uses an open allocation type approach to organizing its software developers.

In the FOSS domain, ready access to version control and platforms like GitHub have further reduced the friction associated with collaboration, and diminished the benefits of being physically co-located with collaborators.

Modularity of the project is a requirement for CBPP to succeed (Benkler, 2006). It must be possible for many individuals to work independently on components which join together to form the product/resource. Where this is true, the benefits of open allocation seem significant.

CBPP also requires a high degree of transparency in organization and decision-making. New contributors must be able to get up to speed quickly on which types of contribution are appreciated or they will likely become disgruntled and quit.

The major limitations of CBPP (and the reason why not all the software we use is FOSS) are:

1. Funding of work, incentives for workers. Most workers need to derive an income from their work, and have limited time to spend on work which is un-paid. Most software is produced within organizations that generate revenue and profit from its sale or deployment - which can be used to pay workers.
2. Important work can be dull. Where a project relies on self-motivated and self-funded participants useful but boring work may go undone and this might hamper the project's progress.

3. Governance without hierarchy. When work is organized along hierarchical relations, it is relatively clear who has responsibility for making decisions and/or there is a method in place to resolve disputes. Lack of direction or lack of agreement on direction can limit a project's progress.

Some blockchain/cryptocurrency projects are addressing these limitations in a variety of novel ways. In the following sections, I will outline how CBPP differs to conventional means of production, and how cryptocurrencies differ to other CBPP efforts.

There is much more to a cryptocurrency than the FOSS which participants in the network run, but many of the other forms of work which go into producing a useful cryptocurrency and giving it value can also be considered as forms of CBPP.

Organizing and Funding Software Production

One of the best characterizations of the difference between proprietary and open-source software (OSS) is Eric Raymond's The Cathedral and the Bazaar. This contrasts the top-down coordination of a large centrally planned structure (the proprietary Cathedral) and an open bazaar where people interact freely bringing their contributions and needs (bugs and feature requests) together in a bottom-up process that tends to produce good software.

Proprietary software is characterized by relations of control. The proprietary software production company aims to limit those who can use their software by imposing certain conditions, such as paying for it (e.g. Microsoft products) and/or storing one's data through a service they provide while granting them permission to use/sell it (e.g. Google/Facebook's products).

When software is not Free Libre Open Source (FLOSS), there is typically some entity which generates revenue from controlling access to that software. Where that revenue is generated by selling licenses to use the software, the business model is quite recognizable as it amounts to selling units of a product. As such, the organization controlling that copyright also has a recognizable form - with departments for marketing and promoting the product, new product development, and protecting against the infringement of the copyright (through legal and/or technical means) which allows the business model to be sustained.

Technical means of enforcing copyright (e.g. Digital Rights Management, or Digital Restrictions Management as Richard Stallman, FOSS pioneer, would have it) always weakens the software product itself. In the best cases, the user experience is compromised in some minor way (like reporting your actions back to a server), in the worst cases, the product becomes unusable in certain scenarios (such as a lack of internet access to periodically check in with designated servers).

A recently popularized alternative to charging a licensing fee to use the software has been to offer a service based on the software. Users do not download and

install (all of) the software themselves, they use it by connecting to servers that are running the software. These servers are owned or leased by the company, which charges a subscription fee to access the service, and/or captures useful data about the users which generate value for the organization or can be sold to other organizations for this purpose. Services that benefit from network effects (i.e. the product benefits from more users e.g. Facebook, Uber) are particularly well suited to this business model.

The point of this simplistic overview is to establish that the question of how software development and infrastructure is funded has become an important one for human society. Software is penetrating many walks of life, and the question of how it is funded is shaping the offerings which make it to the market.

In the proprietary software/data domain, the organizational forms are quite recognizable from the industrial era. In place of functions like obtaining and distributing physical raw materials, there are functions like protecting intellectual property. Whenever more revenue can be generated from more customers it makes sense to invest in marketing the product with a view to increasing its usage. With strong revenues coming in (or the prospect of strong revenues to come) it makes sense to hire staff (or contract out the work) to further develop the software or to develop new software products.

The question of whether to hire staff or contract with external entities to get work done was considered by Ronald Coaese in *The Nature of the Firm* (1937). In this article, Coaese considered why organizations form and hire employees when the production they engage in could be contracted out, when an efficient market would allow for the organization to exist as a nexus of contracts.

There are transaction costs associated with contracting out work, such as finding a reliable supplier and negotiating a fair price, then ensuring enforcement of the contract. At smaller scales, it tends to be more efficient to hire workers and organize their production within a firm, than to rely on the market to serve every need with individual transactions.

In place of transaction costs, the hiring of employees incurs the need to organize them, and associated costs. Coaese argued that the cost of organizing a workforce internally rises disproportionately with the number of transactions being organized - placing an upper limit on the size of firms beyond which it would be more efficient to revert to contractual price-based interactions.

The internet and ICT developments have significantly reduced many of the costs associated with organizing a workforce, and this has allowed organizations to reach new scales in terms of their geographic reach, complexity, and global significance. There are however reasons to believe that over time bloat, inefficiency and misallocation of resources become more prevalent within these large organizations, as suggested by Coase's work.

One of the things that's new about CBPP is that participants have a different motivational profile. They are engaging in the production effort for different

reasons, with the desire to make and share things displacing the profit motive and need to sell labor as fundamental drivers.

Intrinsic Motivation and Extrinsic Rewards

One concept from the Psychological literature relevant here is that of **intrinsic motivation**, which means being motivated by some inherent interest in the task and the satisfaction its completion will bring. **Extrinsic motivation** means being motivated by some external and separable outcome (e.g. getting paid). The difference between intrinsic and extrinsic motivation has been demonstrated experimentally (Deci, 1972) by asking participants to engage in some task like solving puzzles and controlling whether they receive an external reward (they are paid to puzzle) or not. Following the completion of the task, the participant is then ostensibly left to their own devices in the same environment, and observed to see if they continue with the task. Participants who were not rewarded to complete the task tend to spend more time doing it in the subsequent free choice period. This has been interpreted to mean that the extrinsic reward (payment) displaces the intrinsic motivation participants would otherwise have felt (enjoying the puzzles). People who are paid to puzzle feel like they are puzzling because they are getting paid, when the payments stop so does the puzzling.

This experimental paradigm has been used to study how different kinds of extrinsic rewards interact with intrinsic motivation. In a comprehensive meta-analysis, Deci & Ryan (1999) reported that rewards which are engagement-contingent (require participation), completion-contingent and performance-contingent all significantly undermined free-choice intrinsic motivation.

> As predicted, engagement-contingent, completion-contingent, and performance-contingent rewards significantly undermined free-choice intrinsic motivation (d = -0.40, -0.36, and -0.28, respectively), as did all rewards, all tangible rewards, and all expected rewards. Engagement-contingent and completion contingent rewards also significantly undermined self-reported interest (d = -0.15, and —0.17), as did all tangible rewards and all expected rewards. Positive feedback enhanced both free-choice behavior (d = 0.33) and self-reported interest (d = 0.31) the factors associated with diminishing intrinsic motivation.
>
> - Deci & Ryan (1999)

It is interesting to note that the core aspects of many jobs are significant detractors for intrinsic motivation. In order of decreasing severity:

- Show up to work at the required time (engagement-contingent)
- Do your work as expected (completion-contingent)
- Do your work well (performance-contingent)

In general, previous research has found that the undermining effect

> of external incentives is especially powerful for monetary compensations that are perceived to be controlling. The effects are larger for monetary rather than symbolic incentives and for expected rather than unexpected incentives.
>
> - Roberts et al., 2006

Rewards which are mechanistic and entirely predictable detract from intrinsic motivation, but unexpected rewards do not. I interpret this to imply that the more clearly an actor associates their actions with gaining a specific reward the more it dampens their intrinsic motivation.

Positive feedback enhances intrinsic motivation, and is the only form of extrinsic reward that has been reliably demonstrated to do so.

Intrinsic motivation features heavily within FOSS. The desire to make something useful and offer it to all is the origin of this mode of production, and how most people start contributing to CBPP more broadly.

Lakhani & Wolf (2005) surveyed 684 developers in 287 FOSS projects and found that:

> . . . the enjoyment-based intrinsic motivation, namely how creative a person feels when working on the project, is the strongest and most pervasive driver. We also find that user need, intellectual stimulation derived from writing code, and improving programming skills are top motivators for project participation.

They also reported that around 40% of contributors were paid to participate in FOSS projects.

Roberts et al., 2006 have investigated a number of hypotheses drawn from the intrinsic/extrinsic motivation literature, in an excellent study that looked at contributions to 3 Apache (FOSS) projects, using both archival data about contributions to the code and surveying 288 contributors. They found little evidence of extrinsic rewards crowding out intrinsic motivation, but they did find relationships whereby status motivations enhanced intrinsic motivation, and being paid to contribute enhanced status motivations. There was no relationship between intrinsic motivation and level of contribution, leading the authors to suggest that some degree of extrinsic motivation (i.e. being paid) may boost participation by giving contributors a reason to work on tasks which were not the most appealing but had high value for the project.

Contributors who were motivated by use-value (i.e. they were adding a feature they wanted to use, or fixing a bug that was causing them trouble) tended to have lower levels of contribution. The researchers also found that recognition for past performance through rankings boosted motivation, and that this was part of a functioning meritocracy within the Apache projects.

One of the weaknesses of this study was that it focused exclusively on the Apache community, and it is not clear how far the results generalize beyond Apache

to other FOSS projects. It seems likely that the details of how each project is organized and how paid contributors interact with their employers matter a great deal.

In my opinion, intrinsically motivated participants are desirable, especially in the blockchain space - but there are limits on purely intrinsic motivation. Some people (who need to earn an income for their work) are excluded, and the overall level of contributions can be enhanced with well deployed extrinsic rewards like payment and recognition.

The Software Industry

While intrinsic motivation may be a factor in the behavior of company employees, this cannot be assumed. What can be assumed is that the payment workers receive and the importance of that money to them marginalizes any role for intrinsic motivation. The individual's will is subjugated to that of the corporate hierarchy, at least within certain time periods where the employee is "at work".

The lack of intrinsic motivation means that workers may not actually complete their work if they can get away with it, which necessitates means for the corporation to ensure that they get what they are paying for from workers.

Classically this has been solved with the idea that being an employee involves being present in a particular place at particular times and performing tasks within view of an overseer, with further levels in the hierarchy where the productivity of those groups is monitored and directed.

Amazon seems to be blazing the trail here in terms of a digital panopticon that would allow the work of many workers to be overseen efficiently at scale and in detail. A key part of this approach is the use of software systems to monitor and direct workers. Interactions with one's superiors that are largely mediated by a computer algorithm virtually guarantee that the effect on intrinsic motivation will be crushing.

In an office-type context, monitoring whether someone is physically present is not a great way to ensure they are doing anything useful. There are a lot of things you can do on a computer, so knowing that someone is present at their desk doesn't mean that they are doing what they're supposed to be doing, or generating any value for the organization.

It is possible to track what employees use their work-owned computer for to some degree, and to (attempt to) limit access to certain applications (e.g. Facebook, YouTube) from within the organization's network. Allowing employees to carry their own smartphones at work further complicates the issue of ensuring productivity through surveillance and mandated presence.

The use of metrics and personal appraisals of performance as measured against some targets are standard tools for ensuring employee productivity. These

methods do not fit well with software production, which is by its nature highly complex and technical, limiting the degree to which an observer or manager can assess the quality of a piece of work unless they have also worked on the same components themselves.

To take a practical example, the use of "stack ranking" where employees are ranked according to some metrics automatically derived from their code commits (with termination and promotion decisions based on these ranks), was rejected as sub-optimal by Microsoft after use for some time. It is easy to imagine how this kind of work environment would detract from the experience of workers and lead to emphasis being placed on the wrong aspects. The application of a similar approach by Google, although implemented in a less heavy-handed way, seems to have killed the idea of "20% time", a level of discretion around what employees worked on which led to the creation of some of the company's more popular services.

We can think of people who are more extrinsically motivated to work (they work to get paid because they need money) and have an ambivalent relationship with their employer as one end of a scale. At the other extreme are people who derive significant value from their work and for whom it makes up an important part of their identity. The extrinsic motivation of payment, and the desire to increase one's level of status and payment can be powerful motivators - but they are motivators to excel in relation to progressing within the organization, rather than directly applicable to the work. Thriving within the organization can mean compromising on one's own values.

Most employees probably fall somewhere in the middle of this scale, with both intrinsic and extrinsic motivation playing a role. The manner in which organizations reward their employees plays a large part in shaping behaviour. Peoples' quality of life is affected by their income, and they are generally motivated to increase this. If individual productivity is seen to be rewarded within the organization, this can encourage workers to invest more effort in their work.

Decisions about rewards like promotion tend to be made through personal appraisals conducted by superiors in the hierarchy. In this case, the internal politics of the organization are a significant concern for employees, and success might be better cultivated through networking and making a favourable impression on superiors than focusing entirely on the task they have been assigned.

Status and rewards matter to participants, and they will tend to optimize their behaviour to maximize these. The more explicitly the rules of reward/promotion are defined, the more susceptible they are to being gamed, and the more they detract from intrinsic motivation.

The organization is an important entity because it can capture value from the enterprise and enrich employees, contractors and shareholders. Decisions about how the organization's products (like software) are developed are made according to the internal workings of this organization and its top-down hierarchical

relations. People with responsibility for bolstering or maintaining revenue streams typically occupy positions near the top of the hierarchy, and so those concerns can dominate the direction of development and tend to push out the views of the people who work more directly on specific aspects.

The concept of technical debt is useful in understanding how top-down management can complicate the task of producing software and lead to inferior outcomes. In general technical debt means paying an ongoing cost for taking a shortcut and doing something in a way which is faster and easier than doing it "properly". The extra time taken to accommodate this weak foundation in subsequent development is like paying interest on the debt.

Where development is directed at a high level by people who are not directly involved in producing the software, such as by executives who are more interested in business development opportunities and generating revenue, this is more likely to result in technical debt. Working to deadlines for product launches is also likely to exacerbate technical debt as it can force the taking of shortcuts.

The Iterative Capital thesis on what's driving the cryptocurrency phenomenon presents an insightful view of how technical debt arises and the effects it has on software and its developers. This blog post presents an interesting individual perspective on technical debt.

David Graeber's *On the Phenomenon of Bullshit Jobs* (2013 article and 2018 book) considers what constitutes a bullshit (pointless) job, how many people think they have one (~37-40%), how it affects them and the organizations they work within. The book has a section about FOSS development and describes an interesting pattern of integration between FOSS projects and private for-profit companies that rely on their software. Within these groups, the most desirable and highest status work concerns the software's FOSS core (which is commons-based and often not directly compensated). In contrast, much of the work of the organization's employees is directed to "duct-taping" the integration of this streamlined high-quality FOSS core with the proprietary and technically indebted software which the company relies on to generate revenue. The same individuals may participate in both capacities, working on the core FOSS components in their free time and duct-taping those same components in a production environment during their working day.

Graeber's work also offers an opportunity to take a step back and consider FOSS as just one kind of Commons Based Peer Production, and to infer that many of the same basic mechanisms are at work in the production of other non-rival information goods.

Graeber makes the case that over the last decades we have witnessed a proliferation of bullshit jobs that serve no purpose within their broader organizational context or externally, and can be actively counter-productive. Graeber posits that this is closely related to the rise in administrative/managerial positions relative to the rest of the workforce - which can be read as an attempt to maintain productivity through hierarchical control as organizations scale. Within

a large organization where sub-domains are relatively opaque to each other, inefficiency or organizational malfunction is more likely to persist or grow for sustained periods as it may go undetected by the entity as a whole. The status quo is always beneficial for some party, and that party often has the influence to maintain it.

Within a small group of workers, every worker is known directly by a relatively large proportion of the other workers. With some degree of insight into each others' work, an informal reputation system emerges which reflects individual productivity fairly well. As an organization grows in terms of the number of employees, each individual is known by a much smaller proportion of the other employees, and managers may be responsible for more workers than they can know individually. Formalizing interactions between workers is an effort to maintain cohesion across an organization and achieve consistency in its interactions with external parties. The more aspects of a job which have been formalized, the more that job becomes about ticking the right boxes and scoring well on evaluation criteria.

FOSS Production

FOSS starts from the basis of having all of the code on the commons, removing the possibility that anyone can seek to profit by restricting access to it. Anyone is free to use it and build on it, to extend it or turn it into something else. The ease with which a FOSS project can be forked and taken in an alternative direction limits the degree to which users or developers have to tolerate any behaviour they dislike from the entity which is producing the software - whether that's some odious new feature or an order to do something which contradicts one's own preference. There is no copyright restriction that prevents people from forming a new group to take a project in an alternative direction.

People who are paid to work on FOSS projects are still accountable to whoever is paying them, and there are FOSS projects where the dominant versions are more or less controlled by people on the payroll of a particular company. All FOSS projects can be positioned somewhere on a continuum between being entirely voluntary and being motivated largely by payments to contributors.

Many participants in FOSS projects work on them part time and do not need to generate an income from this work. For FOSS projects that are not suitable for enterprise support, and not integral to the operations of organizations that have resources to fund development - most contributors will be working on it part time in whatever time they can spare, independently of whatever they do to earn an income.

Some participants and FOSS projects have found ways to generate an income by offering services tangential to the software, such as support with deploying the software or using it.

Red Hat is an example of a company that managed to generate significant revenue by selling subscription-based support and guarantees about compatibility to businesses that wanted to deploy Linux in their operations. It is however a rare example of an organization that funds itself following this kind of model reaching a large size ($3.4 billion revenue in 2018).

Nadia Eghbal has written an excellent and comprehensive piece on "the unseen labor behind our digital infrastructure" which explores the prevalence of open source code in our digital infrastructure and paints a picture of freely provided commons-based digital infrastructure that is often not being looked after by its main beneficiaries.

The report describes several in depth examples of critical and widely used FOSS which is maintained on a shoestring budget by people who are stretched and typically do not want to spend time trying to secure or administer funding for the effort. The Heartbleed OpenSSL bug is one well known example where widely used FOSS had an undetected significant exploit for a long time. The OpenSSL maintainers were stretched part-time volunteers, and the issue could likely have been avoided with more resources to fund coding and code review.

Eghbal also notes that the ideology of "Free Libre" Open Source Software is less important to many people who have embraced OSS recently. Adoption of FOSS practices is increasingly based on broader recognition of the practical benefits.

More recently, it seems like the disconnect between FOSS utility and funding has been receiving more attention. Initiatives like Formidable's Sauce program allow employees to bill for work they contribute in their own time to open source projects which are unrelated to the company's own interests. This is an example of an organization that gains a lot from FOSS deciding to give something back to support the commons. They are quite rare.

GitHub has recently launched a sponsorship scheme through which open source developers can be sponsored, with GitHub matching the sponsorship received by developers in their first year up to a limit of $5,000. This is conceptually similar to Patreon, which also connects content producers with consumers who are willing to fund their work. In the case of GitHub Sponsors it is woven into a platform which many FOSS contributors already use. These are centralized services, where the operator of the platform acts as a gatekeeper in deciding who can be funded through the platform.

I will consider the ways in which blockchain projects are funded in a later section, this is arguably where most of the innovation in FOSS funding is taking place.

FOSS Governance

The defining feature of FOSS governance is the fact that the product is **commons-based and equally accessible to all parties**. There is relatively little friction involved in forking a codebase and taking two versions of a piece of

software in different directions. The ownership of Intellectual Property (IP), which determines who is allowed to develop and exploit proprietary software, has only limited significance. In FOSS projects IP considerations are typically limited to the ownership of non-vital assets such as names/trademarks, domains and hosting services (i.e. control of servers and GitHub maintainer accounts).

FOSS governance is archetypally a case of a group of developers communicating and coordinating informally following "rough consensus". In some studies of the top 25 GitHub repositories (by star count) from 2016 only one explained how its governance worked in any detail, with 62% saying nothing at all about this. In 2018 the same method was replicated and 5 projects were found to explain their governance processes, and there was a greater tendency to offer a document which was tailored to onboarding new contributors - but still many projects had no description of their governance processes whatsoever.

Governance tends to be an afterthought for FOSS projects, as it only becomes a significant issue if the project reaches a certain scale. When the number of participants is small and everyone knows everyone else, it is easier to resolve disputes. Most FOSS projects never reach a scale where the lack of formal governance causes any problems.

There is a cost to implementing (and documenting) formal governance, and so informal governance is likely much more efficient for small projects. When a project reaches a scale where it it is more likely to have unresolved contentious issues, it is also more difficult to add in a new form of governance, because doing so with legitimacy would require buy-in from all existing participants. One natural way for informal governance to scale is by effectively nominating whoever holds the most sway in the process as a "benevolent dictator for life" - being acknowledged by participants as someone who has the personal authority, usually based on respect earned from their contributions, to dictate the resolution of contentious issues.

In the case of unresolved contentious issues within a FOSS community, the lack of a strong barrier to forking means that it happens fairly regularly. Given that all the code for both forks will remain open source, a fork doesn't have to mean the end of collaboration between the two groups. Beneficial changes can be pulled in from the other fork(s) - although doing so can involve considerable effort. In particular, where the project that was forked from is large and active, keeping up with the changes as a "downstream" fork can be difficult. This piece on the history of Debian and Ubuntu by Benjamin Mako Hill affirms that it is best where possible to avoid a fork because of the increased coordination costs and possible duplication of effort. Hill recognizes significant benefits to forking in the degree of customization it offers, with software "one size never fits all" and with FOSS the capacity to adapt and hone it for a particular use is one of it's strengths. Mako Hill calls for better tools to facilitate ongoing relationships between forks.

The control of funding available to FOSS projects often happens orthogonally to

governance of the software. This is the case when most participants are employed within companies that are users of the software. In some cases the project itself has resources (usually donated) at its disposal, in which case the governance of the organization controlling those resources becomes a significant factor in the project's overall governance. Where a conventional organization holds funds or other assets for the project its governance can be understood as following more conventional patterns, familiar from human history.

Blockchains as FOSS

Blockchains and cryptocurrencies could not exist without open source software. Blockchains rely on the principle that anyone can determine the current state of the distributed ledger themselves from first principles. This requires total confidence that the software which reads the ledger and broadcasts transactions is working as described.

Open source is optimal, and standard, for most use cases involving cryptography and encryption. Many eyes on the source code increases the chances that flaws will be discovered, giving more weight to the absence of known exploits. Conducting development work on the open commons also means it should be harder for the entity controlling the releases of the software to include backdoors which allow them to target specific users.

FOSS fits with cryptocurrency and any other domain where trust is important. With proprietary software, trust can only be placed in the entity which produces the software. With FOSS, trust in the software itself can be cultivated. OSS doesn't automatically mean free of exploits or backdoors, but it means that over time those exploits or backdoors are more likely to be identified publicly, because they can be identified by anyone (not just employees with access to the source code).

For projects that aim for decentralization, it makes sense that the full source code should be accessible to all parties, as this removes a barrier to participation as user or contributor. Control of software copyright is a centralizing force, because by definition that control must be vested in some legal entity, governed by a specific set of individuals.

Blockchains are a distinct sub-set of FOSS projects in that the software "prints money" and facilitates transactions using that money. As a consequence, network effects matter to cryptocurrency projects much more than to other FOSS projects. The purpose of the software is to run one instance of a large distributed network, with everyone who is running that software participating on the same network. This is achieved with a set of rules which allow all the nodes in the network to agree on the current state of the network (or what the correct chain to follow is) - the **consensus rules**. Anyone can join the network at any time, and by applying the consensus rules to the data they receive from peer to peer nodes they will arrive at a shared understanding of the ledger's current state.

Participants in these networks can be broadly categorized as falling into one of two groups:

- Actors who can create new blocks, or who participate in the creation of new blocks. In Bitcoin, these are Proof of Work Miners who run specialized hardware that can efficiently make guesses (compute hashes) to a mathematical problem that cannot be solved any other way.
- Actors who can read the state of the blockchain for themselves and broadcast transactions to the network, known as "full nodes". Full nodes help to ensure that every participant in the network is obeying the consensus rules.

Many cryptocurrency users are not direct participants in the network, but rely on third parties to perform the services of knowing about the current state of the network and broadcasting transactions to it.

It is important to Bitcoin that participation in the network is permissionless (anyone can do it), otherwise the entity that decides who has permission to broadcast blocks and transactions can exert control over the network.

Bitcoin operates in an adversarial context, where there are great incentives to manipulate the distributed ledger. This makes the consensus rules of paramount importance, they are the only way to ensure that only a single chain can persist as the commonly recognized Bitcoin - vital for the distributed ledger to be useful and for the asset it tracks (BTC) to have value. In Bitcoin's case the rules state that the legitimate Bitcoin chain is the one with the most accumulated Proof of Work.

The consensus rules are embedded within the open source software that the networks run on. Thus the developers of that software are responsible for ensuring that the rules as enforced by nodes are as understood by their human operators. The stakes are high, with an exploit in the software potentially allowing for the rules to be broken in such a way that the whole network would lose its value.

With great responsibility comes some power, as the developers who write and release the software that the network's participants use are in effect the only people who can propose and implement changes to those rules.

The importance of network effect and maintaining a community's cohesion around a single version of the distributed ledger makes the governance of blockchain software development fundamentally different to other FOSS projects.

Hard Fork Governance

In a project like Linux or Apache, where there is disagreement on the direction development should take or any conflict that causes the group of people working on that software to split, forking the software is a relatively low cost solution. As the full history of development is open to all, any party can copy the codebase

and start building in a different direction from any point. This produces two versions of the software, and from that point users have an additional choice for which version they would like to use - and the choice of one user does not interfere with the choice or experience of others.

Where the project is supported by an organization, that organization's purpose is usually quite limited, e.g. hosting a website/repository/docs for the project and holding any Intellectual Property such as trademarks. In a community splitting dispute, the faction that controls such an organization may have an advantage relative to a new fork (that must start with a different name and attract its own users) but that advantage is not insurmountable. In a sense it doesn't matter whether the new fork overtakes its progenitor because they proceed as independent pieces of software and need have no further interaction with each other.

Cryptocurrencies can have multiple full node software versions, and these can be either forks of each other or completely independent. Bitcoin has a number of full node implementations, including forks of Bitcoin Core and fully independent implementations. These implementations are constrained by having to obey the network's consensus rules. If one version changes these rules or implements them inconsistently it will lead to the fragmentation of the network (or a "chain split") as nodes running one software version follow a different chain to those running another version. A software update which breaks the current consensus rules and establishes a new rule-set is known as a "hard fork".

Projects other than Bitcoin tend to use "hard forks" as a way to upgrade the software, changing the consensus rules in some way that benefits the network and that the great majority of participants consent to. The chain following the old rules fails to progress because all of the block producers have moved to the "new" network. If enough users stick to the pre-fork rules that version of the network and chain may persist.

A sustained chain split effectively splits the community and userbase for a cryptocurrency. As the chains do not share an understanding of the current state of the blockchain, the users following each respective chain are no longer transacting on a shared distributed ledger.

The best known example of a deliberate chain split is Bitcoin Cash (BCH).

BCH forked off the Bitcoin chain in August 2017, as an attempt to resolve some long-running disputes in the Bitcoin community. BCH favored a larger size limit for blocks to keep transaction fees low, and rejected the activation of the SegWit feature added to the Bitcoin Core implementation.

SegWit was added as a "soft fork", it established new rules to make a new type of transaction possible but did not require all nodes to update their rules to accept blocks with these transactions. Soft forks only require miners to adopt the new software for the amended consensus rules to take effect.

Chain splits and the different types of blockchain forks can be difficult to wrap

one's head around - an article I wrote in 2018 contains a high level overview (following a more basic introduction to concepts like PoW).

Bitcoin has for many years adopted a "no hard forks" approach to upgrades that change the consensus rules. A hard fork is one which changes the consensus rules in such a way that nodes running the previous version of the software will not recognize new blocks as valid. This would pose a particular challenge for Bitcoin. As there are many nodes and they have no established way of coordinating a hard fork upgrade, it would be difficult to deploy a hard fork upgrade without leaving some participants behind on a network following the old rules.

A soft fork upgrade changes the consensus rules by making them more restrictive in some way, these only require the support of a supermajority of miners to be successfully deployed. Nodes that do not upgrade will not be forked off the network, although they may fail to follow the current state of the ledger in some respects.

"No hard forks" has implications for technical debt, as it restricts the options available to developers who wish to upgrade the network. In effect, Bitcoin developers must maintain backwards compatibility with software from 2010 (see here for a list of Bitcoin consensus forks).

Bitcoin Cash Hard Fork

Bitcoin Cash (BCH) was born at Bitcoin block height 478,559 (on 1 August 2017), when a faction of the ecosystem which rejected SegWit and preferred to scale the block size introduced its own hard fork change to the consensus rules. It is interesting to note that the BCH faction were forced to make a hard fork change to avoid the activation of SegWit (which was going to go ahead despite their objection, because it had enough miner support).

From this point onward there were two diverging and competing chains which both had a claim on the Bitcoin brand. This competition spanned all of the aspects which make up a cryptocurrency:

- Competition for hashpower. BCH launched with an emergency difficulty adjustment algorithm as part of the hard fork, a drop in hashpower was predicted (because most mining power signalled support for BTC). The difficulty was lowered and made more dynamic, so that the pace of new block production would be maintained. BCH duly lost the competition to accumulate more PoW than BTC, and the emergency difficulty adjustment caused large oscillations in BCH hashpower speeding up its issuance - and also impacting the BTC chain.
- Competition for recognition. As the birth of BCH involved a hard fork, economic actors (like exchanges and payment service providers) had to decide whether they would recognize this new chain with its different rules, and how they would recognize it. Over time, most economic actors

accepted the rival chain under the name Bitcoin Cash and ticker symbol BCH. In the later failed SegWit2x hard fork attempt (considered here), the choice by most exchanges to label the non-2x chain as BTC played an important role.
- Competition for community and adoption. The BCH fork was accompanied by a splintering of the community around Bitcoin, with some supporters of BCH becoming openly hostile to BTC supporters and vice versa. Some merchants and payment providers chose to only accept one version of Bitcoin and reject the other.
- Competition for developers. Each group of Bitcoin node software maintainers had a choice of whether to adopt the new BCH consensus rules in their software. New developers joining in the effort to build Bitcoin and build on Bitcoin now had a choice of which set of rules and chain to follow.
- Competition in the market. The price and market cap for BTC and BCH was I suspect for most people the defining aspect of the competition. The Bitcoin which is worth more, or which market participants expect to be worth more in future, is probably the one they will acquire. This determines which software to run and which chain to follow.

In November 2018 the BCH chain was deliberately split again, to form BCH ABC (now recognized as the winning BCH by most exchanges) and BCH SV. More recently, the BCH ABC chain split again accidentally when an exploit in the dominant ABC implementation was used to halt that chain - a reminder that maintaining consensus among distributed nodes is hard. At the same time, a reorg was detected which double spent some BCH.

Developers with decision-making power for dominant full node implementations have considerable responsibility in determining how these projects develop - but they cannot act unilaterally, at least in principle. Developers can release a new version of their own software, but it is up to the other participants in the network to decide whether to upgrade to that new version. The degree of power that developers have to push changes varies significantly between blockchain projects, depending on the strength of the other constituencies and the project's social contract.

FOSS for Common Pool Resources

On its own, blockchain FOSS software is of little consequence. With the coordinated participation of a number of constituencies it can become the backbone of a powerful network that can transmit information and value digitally in a way which is resistant to censorship, corruption and subjugation.

Strong public blockchains are significant because they are robust, there is probably no way for an opposing force to stop these networks from functioning. This robustness stems from their decentralization, anyone can run a node anywhere, and for as long as there are at least a handful of these nodes, the blockchain will

persist. For as long as the majority of nodes apply the consensus rules faithfully, *the network will continue to function according to those rules.* The question of how significant blockchains will be depends on how popular they are, but the concept and potential is here to stay, running and using them is now just one way to use the internet.

The blockchain network's capacity to provide this service stems from the way it incentivizes block producers to follow the rules (as defined in the code but also the social contract) and act in the best interests of the network. For Bitcoin, it is the value of the rewards available to PoW miners (block subsidy and transaction fees) which secures the network. Greater rewards means more honest hashpower competing for those rewards, making it more difficult to amass enough dishonest hashpower to successfully attack the network.

This section will consider distributed ledgers as common pool resources, applying the framework of Elinor Ostrom as presented in Governing the commons: The evolution of institutions for collective action. Ostrom's work is concerned with avoiding the tragedy of the commons, and she looks at how groups of people aim to do this in a variety of contexts, looking beyond conventional state and market approaches at successful management of real resources.

Blockchain Development Funding

Of the Bitcoin constituencies referenced above, the motivation or incentive of the developers is most difficult to pin down. Miners are handsomely rewarded for the role they play in securing the network, merchants have built a business which relies on the network to function, and users avail of the service the network provides (or hold their coins in speculation that they will increase in value as more people wish to obtain them and use the service the network provides in future).

Developers may be (and most likely are) intrinsically motivated to participate, in the same way that they typically are with other FOSS projects. Blockchain projects also have the capacity to fund development in some ways which are familiar from other FOSS domains (Software as a Service, patronage and donations), and some which are unique to the cryptocurrency space (appreciation of holdings, ICOs, block reward funding). This section considers the ways in which blockchain development is incentivized and funded, and how those funding mechanisms affect the relationship between developers and the other constituencies. The following section considers the related question of how the blockchain is governed, where the relationship between developers and the other constituencies is a significant factor.

The centrality of the software to the blockchain means that developers will always tend to have some influence over the course its development takes, but the nature and degree of this influence varies significantly between projects. The sense of being part of the team which is facilitating and steering the course of a

blockchain's development is likely a big incentive for participation, irrespective of whether and how that participation is compensated.

Hold while Building

As with other FOSS domains, developers are probably users. In Bitcoin's case, this means that early developers may well have been holders of some BTC while it appreciated in value by orders of magnitude. Developers who held a significant amount of BTC through the price increases may now be independently wealthy and able to continue contributing without a need to generate an income from this or any other activity.

For early developers of a young blockchain project, obtaining some of the underlying asset makes sense if one believes that one's efforts will help to increase its value. This also serves to align one's incentives with the health of the network, and allows one to benefit financially from price appreciation that may be in some part due to one's work.

Developers who do not depend on any external party for an income are in the strongest position to try and influence the development of a blockchain project in the way that they see fit. Dependence on an external party for income may mean deferring to that party's judgement about the direction development takes.

The logic of "buy coins at $Y and invest effort to improve network's utility, increase demand for coins and raise their value to $Y x 10" also applies to organizations. Any large holder of a cryptocurrency is incentivized to see its price increase, and in some cases it may make sense to invest additional resources to fund developers' work. This scenario has the makings of a tragedy of the commons. As every holder benefits equally from price appreciation, each would prefer that the investment to improve utility came from other holders. Such investment may however have some influence payoff, depending on the relationship between the investor and the developers they fund.

Blockstream is a company founded in 2014 by a group of Bitcoin developers with a mission to "build crypto-financial infrastructure based on Bitcoin".

> Blockstream provides funding for the development of Bitcoin Core, the predominant bitcoin network client software.[7] It also employs a large number of prominent Bitcoin Core developers.[8]
>
> The company has raised $76M to date from investors, including venture capital firms Horizons Ventures and Mosaic Ventures. [9][10][11]
> - Wikipedia, 05/26/19

Blockstream's business model is in some ways similar to the software as a service model of companies like RedHat. Blockstream develops the open source software (Bitcoin Core in this case) alongside services which rely on that software and which generate revenue for the company. Where Blockstream is different is

that the services it provides rely on the Bitcoin network, not directly on the software but on the common pool resource that software is used to create. If Blockstream needs Bitcoin to do something new or differently to improve its service, it does not have the same unilateral power to push that change that a company like RedHat has. What Blockstream does have are some seats at the table in discussions about how the Bitcoin Core software should be further developed, in the form of the contributors it employs.

Bitcoin Core in turn has the benefit of community trust and inertia built up over a number of years, making it quite entrenched with the vast majority of Bitcoin full nodes running this software implementation.

In addition to revenue-generating services, Blockstream may itself hold some of its assets in BTC, benefitting from price increases (and suffering from decreases). I do not know if this is the case. Blockstream could also be used by large BTC holders as a vehicle to invest in Bitcoin's development indirectly, hoping to benefit from both the Blockstream equity and the appreciation of BTC holdings.

It is worth noting that Blockstream's efforts to enhance Bitcoin go beyond the Core software and its own revenue-generating products to encompass things like an array of satellites continually broadcasting the entire Bitcoin blockchain. These allow a user anywhere in the world to obtain the data and verify the current state of the chain without even an internet connection (although a connection is still required to broadcast transactions). Investments such as this demonstrate that it is the common pool resource or network that matters, and that the task of improving its utility does not stop at the boundaries of software but can spill over to include the many other aspects which give that resource value.

More recently still, Blockstream revealed that it had been growing its own PoW mining operation since the issue with PoW miners over SegWit in 2017 (see here).

It is this spillover and the degree to which the software is enmeshed in a resource with other important attributes that makes CBPP a useful lens to apply. I will argue below that the path to realizing this technology's potential lies in bringing more of the aspects that give the resource its strength and value "onto the commons".

Looking beyond Bitcoin, there are a number of other significant funding models to consider. I will describe some of these, along with some historical context.

Early cryptocurrencies could be mined effectively with a variety of consumer hardware, in the early days CPUs were sufficient, later GPUs came to dominate mining and later ASICS (specialized chips which only mine a particular set of cryptocurrencies) were developed. As better hardware becomes available, the older hardware quickly becomes unprofitable to use. At the launch of Bitcoin, Litecoin and other early blockchains, mining was the domain of enthusiasts using whatever hardware they had available. The competition to find new blocks and

obtain the rewards was not fierce, and so any dedicated enthusiast could expect to obtain a reasonably large share of the rewards. For very early contributors, all they had to do was set up one or more of their computers to mine Bitcoin and they would be able to accumulate some. There was a technical barrier here too, where a contributor would have the appropriate skills to set up a miner but outsiders (particularly non-technical people) would have found this much more difficult.

As Bitcoin gained recognition and traction, mining became more professionalized, with economies of scale and advances in hardware greatly limiting the degree to which hobbyists could participate beneficially.

For a group of developers starting a new cryptocurrency, there was now no guarantee that they would be able to mine any significant share of the coins before professional miners squeezed them out. By 2018, a new PoW blockchain could have firms with significant investment and hardware lined up to begin mining as soon as it launched (example: Grin). This left developer teams looking to launch new blockchain projects with a choice to either build in a funding mechanism through which they could receive funding and/or some of the coins, or to move to a donation oriented model for funding development.

Donations and Patronage

Donation based funding is familiar from other FOSS and CBPP domains - sustaining projects like VLC media player and Wikipedia (through the funding of the Wikimedia foundation). In the cryptocurrency space, informal ad hoc donations are relatively common. For example, Andreas Antonopoulos (Blockchain educator) received $1.5 million in BTC donations after revealing that he was not wealthy and being mocked for it. Vitalik Buterin (Ethereum co-founder) has distributed some 1,000 ETH donations on twitter. The fact that cryptocurrencies make monetary transfers easy for their users has meant that it is common for people to list donation addresses, and sometimes sizeable donations are made to those addresses.

Monero has a well established Community Crowdfunding System (CCS) which coordinates crowdfunding for development work. Proposals are submitted and discussed by the Monero community, the proposer iterates the proposal until loose consensus is reached about whether the proposal warrants funding. The Core team moves proposals that have consensus support into a "funding required" status, where they remain open for donations. If and when the target amount of XMR is donated, the funds can be released to the recipient once the Monero community agrees that the listed milestones have been met. Monero's privacy means that donations remain entirely anonymous and the recipients of funds do not know where those funds have come from.

In some ways this places Monero developers who are reliant on funding to work on the project in a weak position. For any work they wish to do they must

ensure that it is in line with what the community wants, and also hope that some people want it enough to donate their XMR. From a decentralization perspective, this is quite a strong approach as it gives many individuals the opportunity to make small donations and together fund specific pieces of work, without giving the intermediary (Monero Core team) direct control of significant resources. It may however be subject to a tragedy of the commons, as individual donators do not stand to benefit more than non-donators from their donations.

The Grin project is also donation-driven, and soon after launch a developer posted about their disappointment that a fellow developer's campaign was not being funded. The Grin Technical Council manages a general fund which receives donations and which they spend at their discretion using a 3-of-5 multisig wallet (funds cannot be spent without 3 council members consent) and maintains records of income and spending. The Poloniex cryptocurrency exchange has committed to donating 25% of Grin trading fees to this general fund for one year. Grin seems to have had success funding development since then, striking up other ongoing funding relationships with stakeholders in the ecosystem. Grin is in the process of formalizing the role of the council (now "core team") which manages the pot of donated funds.

Some funding arrangements exist on the boundary between donations and **patronage**. The "Hard Code Fund" is a fund which collects donations and uses these to support the work of Bitcoin developers. As of June 2019 it had collected 50 BTC ($450,000) and was using this to support two Bitcoin developers, who submit monthly progress reports and receive payouts in BTC. The linked article about this story cites a figure of "less than 10 full-time Bitcoin developers", and frames this as an open problem.

The OKCoin exchange launched a campaign to award up to 1,000 BTC in donations to named developers working on BTC, BCH and BSV. OKCoin users can vote for the project they would like to donate to, and each vote awards 0.02 BTC (worth around $200). After one week the campaign's donation total stands at 0.56 BTC, with a total of 28 votes being cast thus far.

Jack Dorsey has announced that Square is looking to fund engineers and a designer to work full-time on Bitcoin and the cryptocurrency ecosystem, as a way to give back to the community. There are some other organizations that have similar patronage schemes in place.

In all of these cases, the donators have some influence over the project by deciding who or what they donate to. The level of autonomy the recipients have seems to be quite high in general, but there is also a chance that stipulations are made in private about what is expected in exchange for a donation or to receive further donations.

Donations are by their nature not a very reliable source of income, because they typically depend on the ongoing generosity of beneficiaries who are external to the production effort.

Premines and ICOs

In recent years, many blockchain projects have been setting up their common pool resource so that it is able to fund its own development, either initially or on an ongoing basis. The remainder of this section reviews the various mechanisms through which a blockchain can fund its own development.

A **premine** refers to allocating some proportion of the tokens before the launch of the network, typically including these allocations in the genesis block when the blockchain launches. Decred is an example of a cryptocurrency with a premine, with 4% of the 21 million DCR total supply allocated to the founders and another 4% airdropped for free to 2,972 participants who signed up following an announcement in the bitcointalk forum. A premine does a reasonable job of aligning the incentives of the recipients with the network, they will only benefit if the assets they received become valuable, which requires the network to have utility and for demand to emerge for the assets. Premined cryptocurrencies place the developers (or whoever received the coins) in a strong and independent position, if the value of the coins increases they may not need external funding for many years (possibly never).

An initial coin offering (ICO) is a form of premine, where the developers effectively sell portions of the premine to other parties before launch (usually also retaining a portion for themselves). ICOs became popular in 2017 with the Ethereum blockchain being used by many new projects to issue tokens soon after the sale but far in advance of the product's launch. Participants in the ICO could then trade these tokens, and many tokens saw significant price appreciation as compared to their ICO price - fuelling the ICO bubble of 2017.

ICOs typically require established legal entities to coordinate them and take custody of and/or distribute the funds received. Such an entity is often established as a not for profit foundation (or conventional for-profit corporation) which has a mandate to spend the received funds on furthering the project's aims.

Ethereum held one of the first major ICOs in 2014, raising $18 million in BTC (31k BTC) in exchange for 60 million ETH. 3 million ETH was allocated to the Ethereum Foundation as a long term endowment, 6 million ETH were allocated to contributors and a further 3 million divided between 8 co-founders. EthSuisse (the company established to conduct the crowdsale) used $2 million of the received funds to pay off loans for crowdsale costs and the remainder to fund development of the Ethereum platform. Ethereum launched as a pure PoW blockchain in July 2015, with inflation funding to reward PoW miners. Writing in May 2019, the circulating supply of ETH is 106 million, so the ICO sale still accounts for the origin of around 68% of circulating ETH.

ICOs tend to reward developers with some of the tokens in an effort to align their incentives with the network, but the entity conducting the crowdsale can make a significant profit even without delivering anything of value, because it receives something of established value (e.g. BTC or ETH) in exchange for the

tokens it grants. This makes it easier to conduct a scam ICO profitably, because the newly generated tokens don't have to become valuable for the crowdsale to pay off for its organizers. At the conclusion of a successful crowdsale, the party which conducted it can already be in a strong position financially regardless of what they subsequently deliver.

The terms of ICOs are typically generous to their beneficiaries, often describing contributions as donations or gifts that come with no obligations, in some cases even renouncing any obligation to grant tokens in exchange for these contributions. For example, the EOS Token Purchase Agreement states that "EOS tokens have no rights, uses or attributes" and that the agreement contributors are entering into is "Not a purchase of EOS platform tokens", purchases are non-refundable and Block.one reserves the right to refuse or cancel purchase requests at any time.

At the conclusion of an ICO, individual contributors and/or a formal organization may be left with significant resources to fund development of the project - sometimes framed as an incentive with a vesting schedule, sometimes framed as a gift with no obligation. This puts the recipient(s) in a strong position to dedicate resources to development of the project, and should incentivize them to do so. It also establishes a particular relationship between the developers who conducted the ICO and the (initial) holders and users of the blockchain.

Individuals who "donated" to the ICO have effectively given money to the party which conducted it in the expectation that money will be used to create a new blockchain. In practice, this gives the recipients of ICO funds particular significance in the governance of the network. If these actors decide to change the rules of the network, other constituencies have a choice of either following the party which is endowed to develop the platform (they may have personally funded this endowment) or follow a network which will become a rival to the one they "invested in" and has no equivalent funding to deploy.

The Ethereum DAO hard fork is a well known example where this was a relevant factor. The Ethereum DAO (Decentralized Autonomous Organization) was an attempt to produce an investor-directed venture capital fund using a complex amalgamation of smart contracts. The DAO was funded by an ICO in May 2016 which raised more than $150 million in ETH tokens (14% of all ETH available at the time), but shortly after launch it was hacked, and the funds were destined to be stolen after a cooldown period expired. Before this cooldown period expired, Ethereum's leaders decided to offer a hard fork to nullify the DAO and return all contributed ETH to where it came from. A coin vote was held in which ETH holders could vote yes or no to this proposition, 87% of those who voted voted Yes but with turnout of only around 8%. The outcome of this vote was used to determine how the new software would be configured - with the default being set to accept the hard fork which undid the DAO.

The hard fork was accepted by some participants and rejected by others, with 15% of the mining power sticking to the pre-hard-fork rules. The Ethereum

Foundation and founders supported the hard forked chain which re-wrote the blockchain's history, those who refused to consent to the rule change ended up on a chain which would come to be known as Ethereum Classic. The Ethereum brand and ticker went to the chain that had development resources, IP and the Foundation behind it.

Block Reward Funding

Some blockchains utilize a portion of ongoing **block rewards** to fund development. In the same way that miners are rewarded for the hashpower security they provide, those who build the infrastructure can also be rewarded for their work on an ongoing basis. This model is good for aligning the incentives of developers (or those who can expect to draw on the development funding) with the long term interests of the network. The funds will accrue over the course of years and decades, giving the likely beneficiaries an incentive to ensure that the network continues to improve its utility and value over the long term. It is difficult to make a fast exit with a large profit.

This kind of ongoing funding also makes the developers more beholden to whatever entity is distributing the funds, likely reducing the degree to which they can act in an unfettered manner to try and impose their will on the network.

With any dedicated source of development funds (premine, ICO, block rewards), the question of who receives those funds or how they are allocated is important in understanding how that network is governed and who has power. As an ICO or premine is a one-time event, funds are typically discharged to the custody of an organization or set of individuals who subsequently follow their own private methods of decision-making about how funds are used.

Ongoing block reward funding is more likely to be paired with a mechanism through which some constituency or set of stakeholders can make ongoing decisions about how those funds are used. There are projects which aim to decentralize the decision-making about how these funds are spent, bringing an important factor that will determine the project's direction and whether it succeeds *on to the commons.* Where development funds are controlled by people or foundations, the way that key entities will act and the decisions they make are likely to be determined in private. For the rest of the participants these entities are autonomous black boxes that exist at the periphery of the commons but have significant effects on its landscape.

In contrast, attempting to decentralize governance means attempting to govern the common pool resource's development on those same commons. This holds the promise of removing some of the dependence on "external" entities. More specifically, it can grant the stakeholders in the common pool resource independence from relying on the specific set of developers who are resourced and incentivized to maintain and improve the network's software infrastructure. The network's independence is achieved through having the means to fund an

alternative set of developers, should the "founders"' decision-making fall out of alignment with what other stakeholders want or perceive to be in the network's best interests.

Bitcoin gamified timestamping and created an open distributed ledger that anyone can transact on, with a method of ordering transactions and determining which are valid that doesn't rely on authority figures. The constituencies which together give the resource value can have conflicting goals, and without established forms of collective decision-making, disputes can smoulder or burn for a long time, occasionally escalating to a hard fork and splintering of the network to give birth to a new chain which would tend to be a fierce rival.

Decentralizing control over how blockchains develop, in a way which leverages the strengths of all stakeholders to the greatest degree possible while maintaining cohesion around a single chain and network, has the potential to enhance robustness and longevity.

The kind of organization and coordination required to cultivate a top-tier public blockchain is not so dissimilar to the kind of coordination required within conventional firms to deliver other software based services. If such a decentralized autonomous entity were to successfully propel a blockchain ecosystem forward, there would surely be lessons that could be applied to more conventional organizations. The running of a cryptocurrency's development effort just happens to be in particular need of decentralization, because the network derives its value from its decentralization.

It is also interesting to consider these organizations through the lens of Coase's theory of the firm - and to look at the degree to which they embrace contracts and the hiring of employees as methods of organizing work. This will be considered in later sections reviewing specific projects, but it is worth mentioning a novel aspect to the distribution of funds here, as it pervades the space (or did so for a time).

The popularity of "Bounty campaigns" in association with ICOs is an interesting example of the use of open contracts whereby any participants who make certain small measurable contributions (e.g. follow on twitter) are rewarded. Such bounty campaigns are usually geared towards raising the project's profile, but they have also been used to incentivize translation efforts by many projects. This kind of approach follows the more general blockchain approach of incentivizing the behavior the project requires from constituents in the expectation that those incentives will attract the required participants.

Common Pool Resources

A Common Pool Resource (CPR) is one which is naturally open for consumption ("size or characteristics make it difficult to exclude potential beneficiaries from obtaining benefits of use") but which is subtractable (faces problems of congestion

or overuse) - the latter point is the key differentiator to public goods.

The tragedy of the commons is a term popularized by Garrett Hardin - it refers to a scenario where an open resource is over-exploited because that is in the best interests of individual consumers, while they have no individual imperative to maintain or preserve the resource. Where the group of resource consumers fail to act collectively to preserve or maintain the resource, the tragedy of the commons unfolds and that resource is spoiled for all.

Some examples of common pool resources are irrigation waters and grazing land, more recently the concept has been stretched to include global resources such as the environment and free digital software/media.

Ostrom was awarded the Nobel Economic prize for observing that the tragedy of the commons can often be avoided through effective governance of the common pool resource. She identified a number of characteristics of successful governance of CPRs, some of which are relevant to blockchains.

Public blockchains are commons-based, in that they are openly accessible and any new node can join the network - but there is a cost to running the network. Bitcoin full nodes must download and process the entire ledger of transactions from Bitcoin's history, and so the data representing an individual transaction has a cost that must be borne by all full nodes into the future. The ability to write to the distributed ledger must be restricted, because otherwise it would be subject to the free rider problem and over-exploited - the blockchain would become so large that high powered servers are required to run full nodes. Bitcoin restricts the size of each block to 4mb, to keep the cost of running a full node low and encourage more people to do so. People who wish to make transactions must include fees with their transactions that the miners can collect, miners tend to process the transactions with the highest fees.

Blockchains have one big advantage as compared to other CPRs - they allow for the rules of the network to be reliably enforced by participants at minimal expense. It is Bitcoin's consensus rules that allow order to be imposed on an open permissionless network. The use of transaction fees to solve the problem of deciding who can make transactions using the limited space is a good example of this, it effectively creates an open fee market, which is a robust low-complexity solution. The use of hashpower competition to determine who can produce blocks (and collect rewards) is another good example of a rule which imposes order on open access.

For physical CPRs it is important to define and know the group of participants or users of the resource, and status can be an important factor in resolving disputes. Ostrom found that it was important to ensure that the community can monitor members' behavior to ensure that the rules are being followed. Bitcoin must operate in an environment where the identity of participants is often unknown, so the rules must be enforced in the same way for all participants.

The consensus rules can be enforced but they must cover every eventuality as

they are the only recourse for dispute resolution. There is, by design, no way to exclude a particular entity from using the resource, so the set of possible participants includes everyone.

Ostrom calls for an accessible low-cost means of dispute resolution - Bitcoin opts to exclude any dispute resolution function beyond the consensus rules.

Ostrom also finds it important that those affected by the rules can participate in modifying the rules. Bitcoin opts to exclude this function in favor of a socially enforced understanding that the rules cannot be changed in any significant way - while allowing the developers (with miner support) leeway to implement backwards compatible changes (soft forks) that add new rules.

It is the nature of software that makes it impractical to set Bitcoin's rules in stone for eternity. Software must be continually maintained, addressing exploits as they are identified at a minimum. For FOSS projects a lack of updates signals death, as failure to patch weaknesses in dependencies as they are exposed will render the software vulnerable to attack.

The changing of the consensus rules presents a particular problem for public blockchains, as membership or participation is determined exclusively by whether one is following the same rules as the rest of the network. If the rules related to the common pool resource are to change, the rule change must be adopted by all participants at the same time, or they will cease to recognize each other as participants on the same network, reading from and writing to the same distributed ledger.

Commons Constituencies

A blockchain's stakeholders can be thought of as belonging to at least one of several different constituencies. Developers provide the infrastructure the network runs on, block producers provide the engine which drives it forward, merchants provide utility (by allowing it to be exchanged for other goods) and users/holders provide oversight to ensure that other participants follow the rules, and demand for the asset, which increases its value. The value of the asset (i.e. exchange rate with other assets) is always important because it determines the network's security budget - how much reward is available to incentivize block producers to participate honestly.

Each constituency has its own role to play in an ecosystem which produces this common pool resource and gives it value. Different projects define the boundaries of these constituencies and set up the relations between them in different ways. The way in which the network develops is determined through the interactions within and between these constituencies.

I refer to these sets of stakeholders of a particular type as constituencies, because it is typically the (strength of) consensus or majority opinion within a constituency

that matters when considering the effect that constituency has on the project's commons.

Proof of Work Miners

PoW miners of Bitcoin are presently incentivized by receiving rewards (newly minted coins plus transaction fees) for each block they produce. The PoW miner subsidy represents inflation which every holder of the asset is indirectly paying for through the relative decrease in the value of their own holdings. Importantly, Bitcoin has a fixed inflationary schedule which will see the rate of inflation drop (half) at specified points in the future, until the limit of 21 million BTC is reached and no more new coins are produced. In principle, PoW miners would at this point be funded by transaction fees only, but there are open discussions about whether that is economically feasible.

The day to day production of the common pool resource is governed in large part through these fees and rewards which incentivize block producers to participate honestly. In a network that relies on PoW miners exclusively for its security, it is vital that these miners do not have the opportunity to collude and adjust history by rewriting a part of the blockchain.

Where a miner or set of miners controls the majority of hashrate in a pure PoW blockchain, they can reorg (reorganize) the blockchain by releasing an alternative chain with more accumulated PoW. This "majority attack" technique can be used to execute double spend attacks. Brief description:

- the attacker makes a transaction (like depositing to an exchange)
- waits for the recipient to accept the transaction (credit the amount and allow it to be traded for something else) while mining on a secret chain that they do not share publicly
- trades their deposit for something else and withdraws that asset
- then releases their longer PoW chain, nodes accept this as the legitimate chain and the first spend is expunged, leaving the exchange holding the bag

There have been a number of double spend attacks on pure PoW cryptocurrencies with lower security spend (and lower market cap). This kind of attack has become relatively common since 2018, with the following blockchains all falling victim to successful majority attacks: ETC, VTC, ZEN, XVG (x3), and BTG.

Bitcoin Cash (BCH) was the subject of a peculiar majority attack which happened during a chaotic period where the network was transitioning to a new set of consensus rules and parts of it had stalled on a forked chain. The hard fork allowed anyone to spend coins which had been sent to invalid (SegWit) addresses on the BCH chain (and were therefore up to that point unspendable by their owner). In practice this meant that the miners who found the first blocks would be able to include transactions claiming these coins. An unknown miner claimed

some of these coins (worth about $1.35 million at the time) but two of the dominant BCH miner pools colluded to reorg the blockchain to rewrite the 2 blocks in which this occurred, and instead claim the coins (and others available in this manner) for themselves.

Bitcoin has to this point never been the subject of a successful majority attack (with the technical exception of a reorg to undo a significant inflation bug early in its history).

In the aftermath of a security breach on the Binance exchange in which 7,000 BTC (worth around $40 million) was withdrawn in a single transaction, a suggestion was made that perhaps Binance could recover these funds by incentivizing PoW miners to reorg the blockchain. The suggested method was to make all or some part of the illegitimately withdrawn BTC spendable by anyone, by releasing key information.

The rationale was that PoW miners would have sufficient incentive to reorg the chain (going back to a point in time when the funds were still in the Binance controlled address) and claim those funds, depriving the attacker of their spoils and discouraging future attacks. A statement from Binance CEO CZ about looking into this caused uproar in the Bitcoin community, and prompted discussion of whether it was practical to execute such an "attack", whether it should be considered an attack at all, and whether it would destroy Bitcoin's value proposition. CZ quickly abandoned the idea upon witnessing the backlash against it, citing concern for Bitcoin's credibility as the primary reason.

These episodes outline aspects of the power that block producers have in blockchain ecosystems. As the direct producers of the common pool resource they may in some cases have scope to bend the network's rules, or at least gain preferential opportunity to execute time-sensitive transactions.

This article by David Vorick provides a comprehensive introduction to the dynamics at play in cryptocurrency mining. One of the most useful ways of differentiating between PoW blockchains and their miner constituencies is by considering the hardware that the miners use. The "default" for PoW mining is that miners use GPUs which are good at computing hashes generally (they have a higher hash rate than CPUs). There is however now specialized hardware available for mining on many PoW blockchains. Application-Specific Integrated Circuits (ASICs) are highly specialized and can only compute a specific type of hash, and so can only be deployed on networks that use that specific hashing function. ASICs are typically so much more efficient than GPUs that once they are deployed on a network at scale they cause the difficulty to increase and make mining on less specialized hardware unprofitable. ASICs push out GPU miners.

ASIC operators have more at stake in the blockchain they mine on because their hardware has limited utility beyond this. The number of blockchains that use the same hashing function tends to be small, and the value they command concentrated. This means that if an ASIC miner were to abuse their hash power to execute an attack on the network they would suffer from any decrease in its

market value. GPU miners are less exposed in this way because the number of alternative blockchains where their hash power can be deployed is much larger. For GPU mined blockchains the amount of hash power available to mount an attack (i.e. not currently deployed by honest miners) is much larger, because this hardware is ubiquitous.

For cryptocurrency blockchains, the security and utility of the resource is indirectly tied to the value of the asset it tracks and in which miners are rewarded. A higher price for BTC means that the rewards for mining can be used to pay for more hardware, energy and shareholder dividends, and this increases the network's security.

Understanding the longer-term maintenance and improvement of the resource is a case of looking at the interactions between the block producers (miners) and the other constituencies that allow for its provision.

Software Developers

Blockchain developers can implement a change to their software which changes the consensus rules, but this will only take effect if the other constituencies apply this update. For some networks, there is only a single viable node implementation, and in those cases the other constituencies have limited choice in whether to accept or reject any proposed changes to the consensus rules. Rejecting a change may mean abandoning the chain which is being actively maintained in favor of a chain whose software is no longer updated, or is updated with weaker quality controls. Where multiple node implementations are available, other constituencies may have greater choice in whether to accept or reject proposed changes. Dominant implementations benefit from inertia and trust, as some participants may choose to defer to the judgement of a group that has already proven itself to be a reliable custodian of the code.

These decisions about which chain to follow blend the political with the technical. The decision of whether to embrace the BCH fork was not just about the merits and demerits of big blocks as a scaling solution, it was also about whether to use software produced by the Bitcoin Core or Bitcoin ABC teams. In an environment where unforeseen issues with code quality can have detrimental affects on utility and value, the developers' ability to produce robust software reliably is a pragmatic consideration.

In pure PoW cryptocurrencies like Bitcoin, miners have to some degree the power to veto a change to the consensus rules proposed by developers. If a majority of miners refuse to update their software to allow for the new rule's implementation, they can effectively block it by refusing to process transactions that rely on the new rule.

One episode from Bitcoin's history involved a showdown between dominant PoW miners and other constituencies of the Bitcoin ecosystem - the User Activated

Soft Fork (UASF). The Bitcoin Core developers coded a new feature (SegWit) which would help Bitcoin scale by relaxing the block size limit and allowing Lightning Network to be used safely. SegWit was incorporated in the Bitcoin Core software along with a miner signalling activation threshold - the change would not activate unless enough PoW miners signalled support for it. This is a common method of deploying Bitcoin soft forks, as they cannot be used without miner support, and this support must be almost unanimous to avoid a chain split. After some months of miners failing to signal the necessary support to activate SegWit, a proposal was made whereby other nodes would force miners to signal support or see their blocks rejected by a significant component of the network. The number of Bitcoin nodes increased significantly, and many of them started to signal support for this UASF.

Ultimately, the PoW miners backed down in this game of brinksmanship, signalling SegWit support before the deadline imposed by the UASF code. If the miners had not backed down, the Bitcoin chain would likely have split in two, with many of the network's "economic nodes" (exchanges, payment and service providers) refusing to accept new blocks from miners which did not signal support for SegWit. If enough miners had stuck to their position of refusing to activate SegWit, their chain would have had the most accumulated Proof of Work (the usual method to determine which chain is the legitimate Bitcoin chain). However, if "the market" had decided to prefer the UASF chain, miners may have lost out economically by mining on a chain whose rewards were worth less. Such a chain split may have damaged the reputation and value of Bitcoin in general, leading to two chains that were in combination worth less than the Bitcoin chain had been before the split - an eventuality which miners (and other constituencies) would wish to avoid.

It is difficult to know how much power the PoW miners really have in a contentious issue, as it depends on how constrained they are when deciding how to use their hashrate. A miner that must sell most of their rewards to meet operating costs has limited scope to mine on the less profitable side of a chain split in pursuit of some political agenda. Such miners are therefore bound to follow rather than set the market's view of the chains' relative worth.

The UASF, BCH and SegWit2x stories from Bitcoin's history illustrate how constituencies other than developers and miners can play a role in determining Bitcoin's future. This is a complex and long-winded process, but to simplify: miners will tend to go along with whatever is most profitable for them, if other constituencies can create a scenario where miners will benefit economically by changing their position and behavior, that is probably what they will do. The abandoned SegWit2x fork was interesting because futures markets (where participants could buy options on coins from the SegWit2x and non-SegWit2x chains, effectively betting on which would be worth more) seemed to play a bigger role in the build-up and ultimate abandonment of the 2x fork.

Bitcoin's history is where we can learn most about these networks, because it has been running for longer and with higher stakes than any other blockchain

project. Some people attribute much of Bitcoin's rise in value to its growing Lindy effect - whereby the longer it survives the longer it is expected to survive into the future.

In recent years we have seen an explosion in the number of projects which 1) aim to use the distributed ledger approach to provide other services, and/or 2) amend Bitcoin's approach to address perceived weaknesses. Writing in 2019, we are at a point where most of these other projects have not been seriously tested, and many have already cracked under duress or withered and died due to lack of interest. The story of the crypto markets over the next decades will be about which projects persist and survive their challenges, developing their own Lindy effects by continuing to provide their service to a high standard.

Proof of Stake consensus

One of Bitcoin's key innovations was to use Proof of Work consensus to allow the processing of transactions to be permissionless - needing only an honest majority of mining power and the right incentives to ensure that the network would behave as intended in adversarial conditions.

In recent years a number of high-profile blockchain projects have launched which experiment with an alternative way of reaching consensus that doesn't involve PoW miners. Proof of Stake (PoS) consensus is based on the idea that holders of the cryptocurrency can, in aggregate, be relied upon to uphold the rules of the network and produce new blocks in an orderly fashion. This article will not explore the strengths and weakness of PoS vs PoW in depth, only highlight the main pros and cons, then proceed to consider how PoS affects the production of the common pool resource.

Pros:

- PoS does not require as much energy as PoW, nodes just need to show that they hold coins to participate, they do not need to solve arbitrary problems.
- PoS is not prone to the same forces that lead PoW mining power to consolidate under the control of relatively few actors (economies of scale and more reliable rewards).
- Holders of the asset should have a stronger incentive to behave honestly, as their holdings would be devalued if the network fails to function in accordance with its perceived rules. PoW miners are more interested in how much they can earn, and may have hardware that allows them to mine on multiple chains (it is common for more than one blockchain to share the same hashing algorithm), decreasing the extent to which their profitability is bound to a specific chain.

Cons:

- Nothing at stake problem. PoW miners continually expend energy to

produce new blocks, when a chain splits they can only direct their hardware to mine on one of the two forks. For a PoS participant who holds the required asset, it is relatively cheap to participate in PoS, and therefore in the case of a chain split one may participate on both of the forked chains. In aggregate, this means that it may prove difficult for the network to reach consensus about which is the legitimate chain, if enough block producers are participating on both chains. PoS consensus networks often introduce security bonds and mechanisms whereby PoS participants can be punished for this kind of behavior.

- Incentivized pure PoS has an inherent "rich get richer" dynamic, because the participants who hold the asset already are the only actors who can benefit from the rewards. The low cost to participate reduces pressure to sell these rewards. The net result is that PoS participants increase their share of the asset while holders who do not participate in PoS pay the cost of being diluted. This could be construed as a kind of rent seeking arrangement, or a form of feudalism.

PoS changes the infrastructure surrounding the common pool resource significantly, removing the miner constituency entirely and giving holders of the cryptocurrency a much larger role. In practice, holding the asset is usually just a qualification to participate in PoS, with the PoS constituency actually being composed of a subset of holders who choose to participate and take the necessary steps. At minimum, this usually means running a node with a wallet open that can respond when called to participate in block creation. Within some systems, participation in PoS may also involve a security deposit, which could potentially be lost if one is found to have violated the rules (by, for example, participating in more than one chain).

Delegated Proof of Stake (DPoS) systems are a form of PoS where holders can delegate the staking power of their tokens to other actors. It is common for DPoS systems to have a fixed number of block producing nodes - EOS has 21, Ark 51, Lisk 101. Where the number of Block Producers (BPs) is fixed, the dynamic is similar to a persistent election in which holders vote to elect their preferred Block Producers (BPs). Tezos uses a form of DPoS where the number of BPs is not fixed, but rather there is a minimum stake (roll size) required to be eligible to bake, and more (delegated) stake means being selected to bake more often (although there are soft limits to prevent overly concentrated delegation).

BPs are the only entities that interact with the blockchain in DPoS systems, so direct control of the network lies with them. BPs are accountable to holders to the extent that the votes/delegations that appointed them can be withdrawn or re-allocated.

BPs are typically rewarded for the role they play in producing and governing the blockchain, to incentivize honest behavior. In some projects, BPs share a portion of their rewards back with the people who empowered them - this occurs openly in Tezos, Ark and Lisk, but was outlawed in EOS according to the original constitution. Sharing rewards with delegators/electors has been

characterized by some as vote-buying or bribery, and decried as weakening the governance of the blockchain. It seems to be the case that BPs compete on the share of the reward they give to voters, but it is not clear how strongly this weighs on the choices of voters/delegators, and whether/which other aspects of the BPs' performance is considered.

BPs occupy positions of power in these networks, they are key decision-makers and also the main beneficiaries of inflation and transaction fees. This makes it possible for cartel type behavior to emerge. Lisk seems to be a good example of this, with two dominant BP factions that each vote for their own members, and make the receipt of rewards by voters contingent on voting for the full set of cartel members.

Some networks extend the domain of PoS to include making decisions about the network's consensus rules - explicitly establishing the constituency of PoS participants as the governors of the network. Decred and Tezos are examples of projects that take this approach.

Governing the Crypto Commons

Considering public blockchains as ecosystems surrounding the production of a common pool resource gives us a framework for considering how they are governed, and how well this fits with their intended purpose. The backbone of these networks is FOSS, a commons-based non-rival public good, but the resource the network produces is a rival good, finite and vulnerable to over-exploitation (without a mechanism like transaction fees which regulates access to the common pool resource).

The developers who write the core software which objectifies the consensus rules, and the entities that can produce new blocks (PoW miners, block producers), are key constituencies in every project. There are also roles for other constituencies in the ecosystem (e.g. users, merchants, layer 2 service providers) to play, with the scale and clout of these constituencies varying significantly between projects. Hard fork based governance where participants choose freely whether to adopt a change in the rules leads to chain splits, which introduces the market (via exchanges) as an arbiter of which chain has greater legitimacy or promise.

This section will consider some blockchain projects that are conducting aspects of their decision-making on the commons. It will focus on:

- the block producer constituency and how changes to the consensus rules are approved and deployed
- the developer constituency, how they are funded and how they relate to other constituencies
- the user constituency, how they participate or are represented in governance

Key considerations:

- to what extent is governance formalized and described?
- what is the role of delegation?
- where a decentralized decision-making system is used, how granular and autonomous is it?
- which aspects of governance happen on chain? where do the other aspects happen?
- how have the blockchain's native assets, or whatever confers voting rights, been distributed, and (how) do they continue to be distributed?

This commons lens has been applied to a number of projects, and the salient points for each project are described on that project's page. It is my intention to apply this lens to every significant project which is at least attempting to expose its governance on the commons, and to build up a resource which answers key questions about these projects in a standardized way.

Before that, I will set the scene by summarizing aspects of Nic Carter's excellent masters dissertation, which reviewed the top 50 projects on a number of dimensions in 2017. 53% of these projects held an ICO, 13% were exclusively PoW mined, 11% held an Airdrop, 9% originated as a hardfork derivative of an existing chain and 4% conducted a premine.

67% of these projects had a token reserve to fund development (ICO funds in many cases) , 10% had community bounties, 8% had corporate funding, 6% had a percentage of the block reward.

In this sample the mean "founder reserve" was 20% and the median 15% (I think this is % of circulating tokens at the time).

> 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.

Another startling feature noted by Carter was the lack of transparency among many projects when it comes to the spending of their development funds.

Looking at a ranked list of blockchain/cryptocurrency projects by market capitalization (e.g. coinmarketcap.com), many of the projects in the top 100 or top 500 are not (yet) decentralized in any meaningful way. Projects that launched with an ICO are particularly susceptible to being controlled by one or two organizations that ran or profited from the token sale, as these are the only entities with funding and a mandate to build the product. In the case of many projects that run on the Ethereum blockchain as a set of smart contracts, this organization also has exclusive privilege to halt or amend the smart contracts.

Decentralization is lauded as the supreme feature of public blockchains, but for

many projects it is still an aspiration. I will only be covering projects which are already conducting some aspects of their governance on the commons, because:

- whatever aspects of governance are not conducted on the commons are opaque to an outsider
- if governance discourse and decision-making is not observable, participation is not permissionless and the process should therefore be considered as centralized
- to say that a project is "not decentralized" is usually perceived as an attack on that project
- where the major players are centralized and opaque entities, there is little of interest for an outsider to observe
- the attitudes and behaviors of participants in the ecosystem matter, to the extent that their constituencies have power - so any planned approach to governance which is not yet in effect has significant unknowns.

Bitcoin

In this section, relevant episodes from the scaling debate in Bitcoin's history are revisited in light of the above framework. It should be noted that these episodes occurred as the resolution of a conflict within the Bitcoin community about how to scale which had persisted for years. The two sides in this conflict can be broadly construed as those who wanted to scale on chain (with bigger blocks) and those who wanted to scale off chain with "layer 2" solutions like Lightning Network:

- The UASF episode demonstrated that Bitcoin's PoW miners do not have unilateral power to veto changes to the consensus rules. The fact that a range of actors in the Bitcoin ecosystem were willing to support splitting the chain, a risky and potentially chaotic move, demonstrates that PoW miners have *some power* to veto changes to the consensus rules which they dislike. In the case of SegWit activation, the miners backed down, indicating that they did not collectively feel strongly enough about SegWit to risk the disruption and damage of a UASF chain split. The UASF side won the game of brinksmanship in this case and did not have to follow through on their threat to fork non-cooperating miners on to their own chain - but it is not clear how the scenario would have played out if the UASF actually went ahead. Without enough mining power or an emergency difficulty adjustment the "BTC forced SegWit" chain would have progressed slowly for a time. If it commanded a price premium relative to the BTC non-SegWit chain then miners may have defected to collect its larger rewards.
- The BCH hard fork and chain split was constructed as a way for a segment of PoW hashing power and ecosystem actors to exit the main Bitcoin chain and strike out on their own. Bitmain, the dominant producer of ASICs and controller of Bitcoin hashpower, was instrumental in establishing

BCH. By establishing BCH as a hard fork which was clearly differentiated from the Bitcoin chain, this approach likely caused less disruption than the UASF would have done. The BCH hard fork also incorporated an "emergency difficulty adjustment" that allowed the chain to progress with significantly less mining power, by updating the difficulty more frequently and drastically. The creation of a forked chain which could persist over time introduced the market as a key force which would determine the eventual winner. Bitmain stimulated demand for BCH by accepting it as payment for ASICs while rejecting BTC, and some other BCH supporting economic actors did likewise. In general though the PoW miners followed the economic incentives and collectively balanced their hashpower between the BTC and BCH chains in whichever way was most profitable for them, following price fluctuations closely. While miners have autonomy they also have costs to cover, and if the market determines that one chain's assets are worth significantly less then it will not be able to support as many miners, lowering its security.

- The SegWit2x hard fork was proposed by a group of 58 companies in the Bitcoin ecosystem in what came to be known as the New York Agreement. This agreement followed a meeting at Consensus in 2017, and much of the opposition which would be voiced focused on the fact that it came from a private meeting which most participants in the Bitcoin ecosystem could not attend, and which was not recorded. It quickly became clear that the SegWit2x fork would be contentious, with enough people opposing it to likely result in a chain split. SegWit2x was abandoned by its main supporters days before it was due to activate, citing lack of support within the Bitcoin ecosystem. The weeks and months leading up to this activation date saw significant volumes of often vitriolic opposition to SegWit2x voiced on social media platforms, and also the trading of 2x and no-2x futures on a variety of exchanges (SegWit2x futures had been trading at $1,300 or around 20% of the BTC price).

Each of these (prospective) chain splits required software to be written which would implement the changes that cause the split. Furthermore, each prospective diverging chain would need its own group of developers who could maintain and enhance the software.

The ultimate failure of the SegWit2x fork occurred not when it was abandoned by its main supporters, but when the small number of actors who tried to launch it anyway found their nodes stuck on the block before the fork was supposed to activate, due to a bug in their code. Another demonstration that skilled and dedicated developers are a necessary part of any plan to fork (or found) a blockchain.

The BCH chain went on to split again and form BSV, then encountered some bugs of its own that caused disruption around a planned hard fork upgrade. It also seems that the dominant BCH miners were able to coordinate a double spend attack while this was happening.

When a fork occurs that results in two chains that share the same hash function, miners can switch between these at will but must at any given moment in time decide which chain to mine on. The chain with minority hashpower in this scenario is more vulnerable to attack because miners who rely on the dominant chain for their income do not have such a vested interest in the health of the network with lesser value. Where opportunities arise to extract profit for the miner at the expense of the network's health, these are more likely to be taken when the miner can make a low friction exit to mine a different chain without suffering economic consequences. GPU mined coins also suffer from this effect generally.

This article by Nic Carter considers this weakness from the perspective of final settlement, or knowing when a transaction has enough confirmations to be considered irreversible. Carter concludes that GPU mined chains can only provide weak assurance that a transaction will not be reversed because it is always possible that significantly more hashpower could be added to the network and the chain could suffer a deep reorg. Blockchains mined with ASICs have a much lower limit on the amount of additional hashpower that could be deployed on the network.

Developer groups must also choose which side of a chain split to join, and for developers this may be a high friction decision where it becomes difficult to switch to work on software for the other chain.

The Bitcoin Core group of developers, whose software is used by 97% of the Bitcoin public nodes, were as a collective on the "winning" side in each of these episodes. It is not clear from the outside whether Bitcoin Core lost contributors who went to work on software that was supporting a different chain.

In the case of a chain split, holders of the asset have an equal number of units on each chain, and now have a choice about which one to use. From a technical perspective, users are not compelled to pick a side. As long as precautions are taken to make transactions incompatible between chains (to avoid replay attacks), users should only be exposed to damage from a chain split to the extent that the two split chains are weaker than the former sum of their parts. Nevertheless, the Bitcoin community did appear to fragment as a result of the episodes described above, with many members announcing their preferred fork and becoming hostile to supporters of the other variants.

Exchanges have some work to do to accommodate the existence of a newly split chain and ensure that their systems handle it appropriately - but they also stand to benefit from collecting trading fees on markets that allow the assets (or futures) to be traded against each other.

The Bitcoin Core developers conduct a significant degree of deliberation about the project in public spaces like mailing lists, GitHub, and logged IRC channels - and as with most FOSS projects the work itself and coordination around it happens quite openly. Discussions about these decisions percolate out into social media more broadly (blogs, twitter, reddit), where a more diverse array

of ecosystem participants make their perspectives known. This kind of public review process is integral to Bitcoin, as can be seen in the rejection of SegWit2x based in some part on how the proposal originated from a closed meeting. Due to its CBPP roots, Bitcoin has a degree of transparency in its governance that far surpasses any other organizational form producing a public resource on this scale - thinking here about private corporations, non profits, government departments and central banks.

Bitcoin's governance is largely informal, as with many CBPP projects. There is however a commonly accepted method of tracking proposed changes to the software - Bitcoin Improvement Proposals (BIPs). I have written about this approach elsewhere and won't repeat it here, suffice it to say that there is considerable discretion on the part of key contributors in determining whether a BIP advances.

Bitcoin Core contributors also communicate in publicly accessible mailing lists, in IRC chat rooms (with weekly meetings that are logged and summarized), and on the Issues and Pull Requests of the Bitcoin GitHub repositories.

As the network grows in significance, the stakes get higher - strategic decisions about the Bitcoin Core software are arguably the most important of any FOSS project. The lack of formal governance means that resolving disputes can be a long drawn out affair, as ad hoc signalling mechanisms may produce conflicting signals and are all susceptible to manipulation.

- Resources
  - Jameson Lopp's Bitcoin resources page
  - Hasu's Unpacking Bitcoin's Social Contract

Ethereum

Ethereum is similar to Bitcoin in that it utilizes pure PoW consensus, but Ethereum has since its beginning planned to switch to Proof of Stake (PoS) consensus. While Bitcoin's developers and ecosystem prioritize stability and conservatism, fundamental changes to how the network operates in an effort to adapt and improve are an accepted part of Ethereum's approach. Ethereum's developer constituency is strong as a consequence. Ecosystem participants understand that the common pool resource is still under construction and that the people building it need a relatively free hand to make changes.

Ethereum's leading developers make an effort to engage in consultations with other constituencies when making decisions about how the network develops. The Dapp developer constituency is large and particularly important, as Ethereum is designed to be a platform which supports a wide variety of use cases, introducing significant complexity and the need to ensure that any changes don't break existing smart contracts.

Developers also make changes to the consensus rules which affect the monetary

policy governing the ETH asset. When Ethereum launched it incorporated a "difficulty bomb" that would force a transition away from Proof of Work after a certain point in time by increasing the difficulty so that it became harder and less profitable to find new blocks. This was presumably included as a way to control the PoW miner constituency and avoid a situation where they veto the deployment of a change to consensus rules which makes them obsolete. Ethereum's developers have on a number occasions amended the consensus rules to move the activation of the difficulty bomb further into the future - because the PoS system is not ready for use.

In August 2018 the Ethereum core developers decided to drop the block reward from 3 to 2 ETH per block - the decision appeared to be formalized on an openly broadcast conference call, following a lengthy discussion phase on social media and previous conference calls where miners had spoken. Such a change is against the interests of miners, who would have preferred to continue receiving larger rewards, but the developers were able to make it and see it go into effect as part of the Constantinople hard fork some months later.

Ethereum is also in the process of switching its Proof of Work function to ProgPoW, with the intention of limiting the effectiveness of ASICs for mining ETH. This represents an effort to look out for the PoW mining constituency that has been with Ethereum since it launched with a hashing function that was intended for GPU mining (to allow for broad participation). In a sense, the rest of the ecosystem has decided that certain miners are more desirable or legitimate than others, and that the rules should be amended to favour these miners.

The DAO hard fork was considered above, in which the Ethereum core developers supported a hard fork to the network to undo a major hack that saw a significant proportion of ETH stolen. Core developers have since then made a point to emphasize that such rewriting of the rules will not happen again. In November 2017 a bug with the Parity multi-sig wallet contract was triggered which left wallets using this feature inaccessible - freezing around 500k ETH (worth around $169 million at the time). Affected parties have since been lobbying for a fix that would allow these funds to be recovered, and come up with an Ethereum Improvement Proposal which would allow the ETH to be reclaimed by its owners. However, deploying this change would cause a hard fork, and there are enough ecosystem actors who oppose this change that it is likely the Ethereum chain would be split into two chains that both persist. It is interesting to note that one of the parties most affected by this issue is Polkadot, an interoperability platform which could be viewed as a rival to Ethereum.

Signalling votes have been held by the Ethereum community in relation to the DAO hard fork, the Parity rescue proposal, the adoption of ProgPoW, and other changes. These votes allow ETH holders to vote with their ETH to signal the course of action they would prefer. They have no formal role, tend to have limited participation, and it is not clear how much weight the core developers place on them.

Vitalik Buterin and Vlad Zamfir have both written about the subject of blockchain governance, in opposition to any method of project level decision-making that involves binding votes weighted by coin holdings. Zamfir has this to say about Ethereum's governance:

> ... the Ethereum governance process are not very well documented, and it's hard to understand them without actively participating in them. They evolved over time, and are not an institutionalization of a formal model, and therefore have no inherent reason to be easy to identify or communicate.

This kind of ad hoc governance worked out on the fly by whoever is participating is a standard FOSS approach. Ethereum has many developers working on its core software, supporting services, and Dapps. In the Ethereum ecosystem these developers are working with shared tools on the same commons, and their discussions are the loudest thing in the ecosystem. As the kind of decisions being made are often highly technical in nature, it makes sense that non-technical people are excluded from these decisions. However, the same process is applied when the questions concern scenarios where a particular party stands to gain or lose, like whether miners' rewards should be decreased or whether a group should be allowed to deploy a hard fork patch to unlock 500k ETH.

Although Ethereum, like Bitcoin, makes an effort to conduct its decision-making openly - when those decisions are made in meetings of developers most people are necessarily excluded from direct participation. The Ethereum developers make a deliberate effort to listen to the project's stakeholders but ultimately they will make a decision about what's best for the network in consultation with trusted peers, as a kind of technocratic council. Other participants in the Ethereum ecosystem implicitly support this approach to governance by deploying consensus-changing upgrades as and when the core developers release them. In principle this means that ecosystem participants actively consent to changes in the rules, in practice they have a choice between going along with what the core developers want or being forked off the network onto their own chain (which dies without enough ecosystem support). The ETC fork has already established a precedent that the "legitimate Ethereum chain" can be whatever the core developers want it to be, not necessarily the chain which preserved the rules as they were previously agreed.

The Ethereum project's leaders are probably right in that on chain coin-weighted stakeholder governance would not work well for Ethereum - because the project has significant technical hurdles to overcome before it can achieve its aims, and because the distribution of ETH is problematic for this purpose. 68% of all ETH in circulation came originally from the ICO, and one of the major forces redistributing it has been ICOs run on Ethereum, which put ETH in the hands (wallets) of the founders of other projects, some of which compete directly with Ethereum.

Within the Ethereum ecosystem, Consensys is a significant corporate entity.

Founded by Joseph Lubin (an Ethereum co-founder and COO of EthSuisse) in 2015, Consensys is a company that develops the Ethereum ecosystem and Dapps. It employed more than 900 people in 2018.

The Ethereum Foundation, mentioned previously, is also a significant entity. Lack of transparent reporting means that it is difficult to know how significant a player EF is in terms of funding - but a report published in May 2019 stated that it controlled 0.6% of circulating ETH, which would have been worth around $40 million at the time.

There are no doubt other significant corporate entities in the Ethereum ecosystem. I do not intend to make an exhaustive list, the purpose of mentioning them is to note that the presence of companies with (some degree of) conventional hierarchical control will complicate informal governance in ways which may be difficult to see. Employees of these organizations and those who want to maintain their favour are unlikely to oppose them (or the people who are seen to represent them) in contentious issues.

Despite the presence of organizations like the Ethereum Foundation and Consensys, and the sporadic donations from Vitalik Buterin on twitter, funding of development is a subject which is actively discussed in the Ethereum ecosystem.

This Ethereum Improvement Proposal (EIP-2025) proposes adding 0.0055 ETH per block to a fund for supporting development of the Eth 1.x chain (as the attention of well resourced parties is more on Eth 2.0 development). These parties would receive a loan for a certain amount and the block rewards (17,050 ETH over 18 months, $3.75 million at July 2019 price of $220) would go towards paying back this loan. The EIP lays out how this loan would be distributed between a number of initiatives.

With this kind of EIP that proposes something non-technical (like changing the issuance) it is, in my experience, very difficult for someone who is not an insider to know what the chances are that it will come to fruition and make it into one of the hard fork updates. The only way I have found to follow this is to watch what influential figures in the community say about it. According to Vitalik Buterin, this one seems to have little support.

Moloch DAO is another initiative for funding the Ethereum ecosystem, it will be considered in the section on DAOs. I mention it here because it has funded Gitcoin and is one of the more high profile funding initiatives on the Ethereum commons.

Gitcoin and Radical Liberalism

Gitcoin is a platform which aims to connect people with skills and desire to work on FOSS projects with people or organizations who have a need and resources to fund the required work. At its core is a bounty type approach where jobs are created with prospective payouts available to whoever completes them, but

there are also other mechanisms through which people can receive funding (e.g. grants). Gitcoin distributes funding in the form of cryptocurrency.

Gitcoin seems fairly closely allied with Ethereum, with the "Labs" product described as "Experiments to grow Ethereum". One of these experiments has been in deploying the principles of "liberal radicalism", specifically quadratic voting, to fund 25 Ethereum infrastructure projects. This post outlines how the experiment was designed, it can succinctly be described as "crowdfunding with matched donations", where the entity matching the funding weights its matching contributions more towards the projects which received many smaller donations. In this case Gitcoin had up top $25,000 to award in matching donations.

This kind of quadratic voting is intended to strike a balance between giving people who have or contribute more greater say, but according to a quadratic rather than linear relationship (if A donates 10x more than B, they get more influence but not 10x more influence). The concept is drawn from the book Radical Markets, which Vitalik Buterin has expressed support for - co-authoring a post with the Radical Markets co-author Glen Weyl where Buterin states that they would be interested in applying the concepts to Ethereum.

The report on the experiment with this approach on Gitcoin suggested that collusion had taken place to distort the outcome. The difficulty in applying this kind of approach in the cryptocurrency context is its weakness to sybil attacks (where an individual can operate many accounts to appear as many individuals). Given the pseudonymous nature of cryptocurrencies and ease with which new wallets or addresses can be created, it is difficult to establish how many individual humans are represented in any set of wallets or addresses. Approaches like quadratic voting rely on being able to differentiate individuals (so that their influence can be weighted accordingly). It is usually not possible to do this within a blockchain ecosystem, and the capacity to reliably identify individuals would itself be a radical change for most blockchains - which some constituents would object to.

Gitcoin is one of many interesting examples of novel approaches to solving the problem of FOSS infrastructure funding, but it does not itself have a firm funding model yet, and is currently exploring its options (which seem to include a token sale). There is an open EIP (1789) from a Gitcoin co-founder Kevin Owocki which proposes that inflation funding (20% of issuance) be allocated to Ethereum "ecosystem stewardship".

Gitcoin and the "RadicalxChange movement" is a good example of experimentation with new economic models in the blockchain context.

Blockchains would appear to be ideal laboratories for experimentation with approaches to governance and economics, with their capacity to apply rules rigidly and all the problems of an emerging technology and mode of production to solve.

Monero

Monero is a privacy-focused PoW cryptocurrency with no formal governance that makes regular hard fork upgrades. These hard fork upgrades include technical advances (like bulletproofs, which decrease the on chain footprint of transactions) and also changes to the hashing function.

The changes to the hashing function are made in pursuit of "ASIC resistance". When there is evidence which suggests that ASICs are active on the network, the hashing function is altered to make those ASICs obsolete. The Monero community is committed to the ideal that users of the network should be able to mine XMR, and see reliance on specialized hardware as a weakness. Conversely, there are sound arguments that this will result in weaker security because of the much larger pool of potential hashrate that could be deployed to attack Monero.

The first time the hashing function was changed, a number of split Monero chains formed, most of which maintained the existing hashing algorithm. These forks have limited usage and low prices, some of them may have been instigated by the producer of Monero ASICS (which would become significantly less valuable after the change to consensus rules).

Monero is itself the result of a hard fork to the Bytecoin blockchain. Bytecoin was the first cryptocurrency to use CryptoNote, and when it emerged that the developers appeared to have premined 82% of the total supply (while faking dates on blocks and a whitepaper) many forks appeared. Monero was the most successful survivor.

Hard forks are constructed by the Monero Core team following a rough consensus approach. Core developers participate in logged IRC meetings monthly.

In relation to funding of development work, Monero has one of the best-developed donation-based approaches, the community crowdfunding system (CCS, previously outlined in the blockchain development funding section). This approach has the advantage of not overly centralizing control of development funding. There are key people who make decisions about what the consensus is, but they don't have direct control or discretion over funds. The key action of donating XMR towards specific project budgets is permissionless, relying on the generosity of unknown external beneficiaries.

Reliance on short-term grants from unknown beneficiaries is not without problems. Income security is generally desirable for workers, and the lack of this security may exclude some people from contributing.

The Electric Coin Company, which founded Zcash and is receiving a significant proportion of 20% of the ZEC issuance for the first 4 years, offers a stark contrast. During the currently unfolding kerfuffle about Zcash funding, the ECC stated that it required a minimum of 1 year's notice about whether new block reward inflation funding would be available after the "founder's reward" expires, or else they would have to start looking into other revenue sources. The Zcash section

has more information about this.

Writing in August 2019, the new version of the CCS has been live for almost 1 year (~11 months), there have been completed proposals which were paid out ~1500 XMR, worth $120,000 at today's price of $82. Work is in progress on a further 15 proposals (where the XMR has already been provided and is being held in escrow) - worth ~4600 XMR or $2.1 million at today's prices. Raising this kind of money through donation campaigns is an impressive feat, but the volume of funding passing through Monero's community crowdfunding system is relatively low compared to the funding enjoyed by some other projects.

EOS

EOS uses a Delegated Proof of Stake (DPoS) system in which token holders vote with their tokens to elect 21 Block Producers (BPs). EOS BPs must run nodes that have relatively high specifications to participate in block production - this is fundamental to EOS' solution to scaling and allowing a large number of transactions per second.

The EOS token was originally an erc-20 token on the Ethereum blockchain, issued to participants in a year-long ICO which raised $4 billion for Cayman Islands startup Block.one.

The EOS mainnet launched in June 2019, after a few false starts and generally hard time, with security issues uncovered by audits and phishing attacks on Block.one's email address book.

The best resources I have found which describes the BPs and how they are rewarded are this infographic by Steve Floyd and this FAQ by Ben Sigman - the details are also in the EOS technical whitepaper, in much longer form. EOS BPs are rewarded with inflation funding, with the supply of EOS increasing by 1% each year and BPs sharing these rewards. 75% of the inflation rewards are distributed according to the BPs' share of the voting power, with the remaining 25% being reserved for the top 21, active, BPs. The BPs not in the top 21 are referred to as "Standby" BPs, but there is no enforcement of the idea that they should have nodes ready to participate in block production. There is a minimum threshold for BP rewards, and presently the top 80 BPs are receiving EOS each day (minimum amount is 100 EOS, worth around $360 - average top 21 reward is around 800 EOS, worth around $2,900).

When 15 of 21 active BPs agree to change the consensus rules, they can coordinate the activation of the change between themselves. Beyond changing the consensus rules, the BPs can coordinate to achieve specific aims.

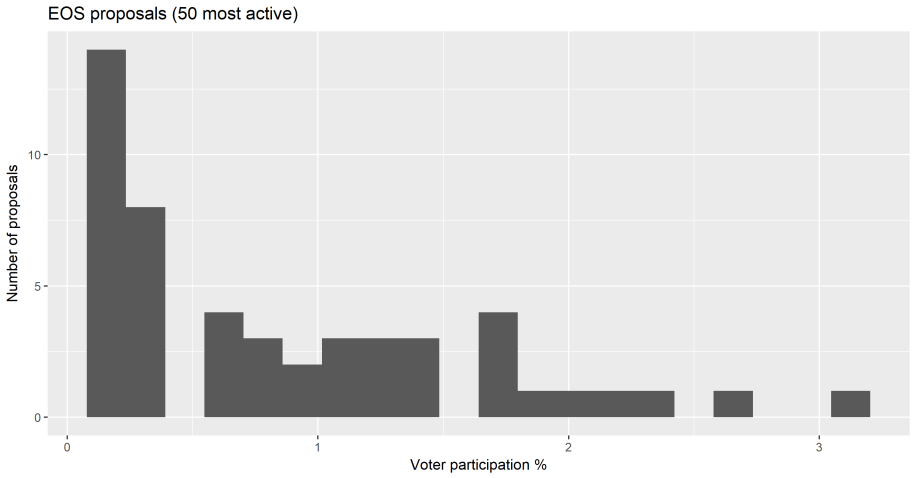
An example of this occurred shortly after EOS launch in June 2018, when the EOS Core Arbitration Forum (ECAF) responded to complaints of private keys being stolen by ordering BPs to freeze 27 accounts. The BPs coordinated to freeze these accounts by agreeing not to process transactions from them, and

maintained this freeze-out until February 2019, when a newly active BP was rotated in and did not apply the blacklist, allowing some of the funds to be moved.

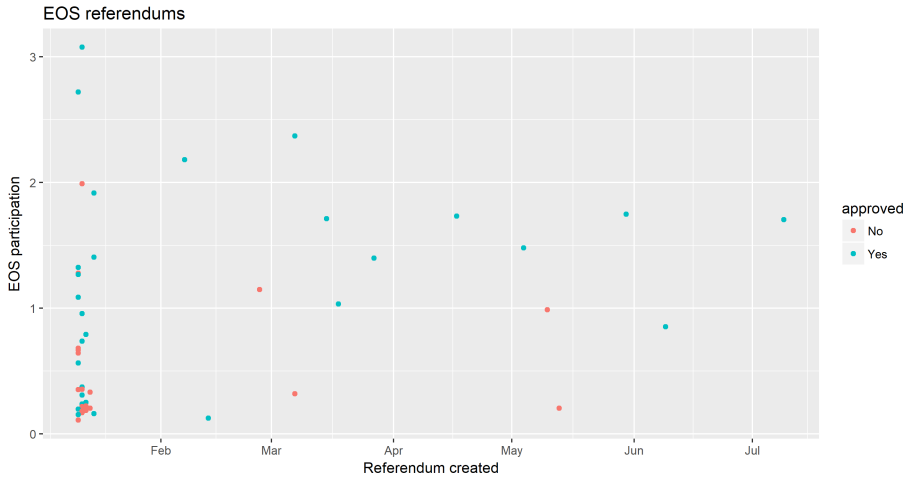
This locking of accounts proved controversial, as it was not clear how the ECAF would resolve the disputes, and the EOS community appeared to lose enthusiasm for such arbitration. The ECAF had been part of the EOS constitution, a document outlining rules for participation in the network which all users and BPs had to agree to. The constitution also had other rules which presented issues with enforcement, like rules against lying and vote buying, and soon after launch Block.one made it known that they were looking to replace the constitution.

The EOS constitution also called for a referendum tool through which EOS holders could vote directly on issues related to the network, with the idea being that the BPs would implement these decisions if they met a quorum requirement of 15% EOS voting and 10% more voting Yes than No.

EOS referendums went live in January 2019, and saw an initial burst of activity, but the proportion of circulating EOS that votes in these polls is low (maximum of 2-3% of EOS voting) and has dropped over time. For the 50 referendums with the highest participation, the mean is 0.9% voter turnout.



For this analysis I have only included the top 50 referendums by turnout, data from EOS Authority. There have been around 200 proposals in total according to EOS Authority, but many of these are effectively spam proposals with no votes (there are some Lorem Ipsums in the mix). There is no fee to submit a referendum poll and no gatekeeper to filter out spam. One of the more popular referendums suggests adding such a fee.



As this scatterplot shows, much of the activity around EOS referendums occurred in January 2019, soon after the tool was launched. The proposals with the greatest turnout were submitted in January, and all of the proposals with 2% or greater participation were submitted by end of March. Only 7 of the most active 50 proposals were submitted in April-July 2019.

I am aware of two actions the BPs have taken which were in line with referendum results: replacing the Constitution with a new User Agreement, and burning the accumulated WPS funds.

In April 2019 the EOS constitution was replaced with a new user agreement, proposed on chain by EOS New York and approved by the 21 Block Producers. This change had been put to EOS holders in a referendum, which had 99% approval but only 1.7% turnout at the time when the BPs enacted it.

In May 2019 EOS Block Producers burned 34 million EOS (~$272 million) from the eosio.saving account. These funds had accumulated from the 4% inflation which was to be used to fund project development through a Worker Proposal System. This idea fell out of favor with the EOS BPs and community, and 15 BPs supported the proposal to burn accumulated savings on May 8. New tokens are still accumulating in the savings account, but this seems likely to be removed as there is an open referendum to remove the 4% inflation for development entirely, which has almost unanimous support from around 2.7% of EOS tokens that have voted.

Of the 50 top proposals, 29 have been "approved" or are on course to be approved, based on a supermajority criteria of the yes - no score being larger than 10% of the total voting stake. The original EOS constitution defined a quorum requirement of 15% participation of EOS tokens, so by this measure none of the proposals would be considered approved. The BPs have enacted 2 decisions in line with referendum polling, but it is not clear how many of the other 27 referendums with positive outcomes will be enacted. I think it's fair to say that

referendums don't play a large role in EOS's governance.

I am not aware of any public platforms where significant discourse about EOS governance takes place. There is a Telegram channel where Dan Larimer occasionally comments, and these comments are posted to reddit. I'm not going to count them but it seems like a lot of the top posts on /r/EOS are quotes of things Larimer has said on Telegram or Twitter.

The EOS Block Producers provide some of the better EOS governance resources and discussion spaces, and often release statements about what is happening on the network. There are a number of BPs which provide platforms for viewing and participating in EOS referendums. I used EOS Authority's referendum page to collect data for the top 50 proposals by turnout, as it has the most comprehensive metadata for proposals. There is a space for comments on each proposal but the comments tend to be short and few.

The referendums themselves are on chain. EOS is addressing the market for high throughput and capacity blockchains, and so the capacity required to host referendums on the EOS blockchain is not a significant factor.

Although the referendums are on chain, they are somewhat peripheral to the EOS ecosystem, with limited participation and attention, and any discussion being fragmented across a variety of platforms.

The election of BPs is the most important aspect of EOS governance, and whales holding large EOS balances dominate this process. This video looks at the breakdown of BP voting and identifies 14 whales that dominate proceedings, with every BP in the top 21 having support from at least 4 of these whales. Among these whales there are two that stand out as having as much EOS as the rest of the whales put together - the Bitfinex and Huobi exchanges, and two factions have formed of whales that tend to vote with either of these large exchanges.

It is interesting to note that these exchanges are playing a major role in EOS governance with what is in some part their customers' EOS. This dynamic likely negates much of the skin in the game advantage of token-holders as a constituency - with the exchanges not having the same incentive to look out for the health of the network. Exchanges which run major BPs also collect significant rewards from this activity.

Bitfinex for its part does make some effort to relay the voting wishes of its customers with the stake it controls.

The power of EOS BPs will depend on how actively token holders follow BP performance and change their votes to elect new BPs. The protocol actually incentivizes this by applying a decay function to vote power whereby votes would start to lose their power if not refreshed weekly. As of August 17th 2019 there is 52% of EOS "staked" but the effective voting power is only 34%, so many EOS voters are not voting at their maximum capacity because they are not refreshing their votes often enough.

It is difficult to ascertain the reasons why token holders vote for some BPs and not others, and how much thought goes into these decisions. A supermajority of 15 BPs is however enough to control the EOS blockchain, and the number is small enough that coordination is little obstacle.

Block.one occupies a dominant position in the EOS ecosystem, with the BP/user constituency having effectively paid them $4 billion to develop the EOS.io software. Block.one has the resources to push EOS development in the direction of its choosing, and can shape the broader ecosystem through its VC investments.

All EOS tokens in circulation were either bought in the ICO or produced through inflation by the Block Producers (who were elected by the ICO holders). People who wish to use EOS must obtain tokens, which ultimately all come from these two sources. In this model the founders and initial ICO participants effectively own the network because they built it, and other parties must buy or lease tokens to make use of it. As of June 2019, 98.4% of the EOS tokens in existence were created in the ICO.

Tezos

Tezos uses Delegated Proof of Stake (DPoS) consensus, but does not put a cap on the number of BPs ("bakers") - they refer to this as liquid proof of stake. In principle the maximum number of bakers can be quite large, it is determined by the minimum "roll size", but bakers that control more XTZ (Tezos' native currency) will bake more blocks and have a more reliable income.

Tezos is built around a process for amending the protocol (rules of the network) in which bakers vote over a series of phases to select, test and apply a set of changes to the protocol. Baking nodes all follow the outcomes of these votes to decide which version of the protocol they should run, in what has been described as a self-amending protocol. On Aug 29 Tezos launched its Agora platform, which tracks the outcomes of current and past protocol change cycles so that stakeholders can follow this. Agora also links to a forum post for each proposal where it can be discussed, this is a new feature and so far none of the proposals have significant discussion.

For Tezos the constituency of bakers (there are currently around 240 bakers per cycle, number taken from this chart at cycle 140) is charged with producing new blocks and also with deciding what the rules of the network are. Holders of XTZ can delegate their stake to a baker of their choosing and bakers typically share a portion of the rewards they receive back to the delegators, less a fee of ~5-33%. Holders who delegate their XTZ have no formal role to play in the network, bakers are the key actors who produce new blocks and make decisions about consensus rules. If a holder has enough XTZ for at least one roll, they can participate in baking directly (but would expect to be selected to bake and receive rewards sporadically).

Delegation allows a high proportion of XTZ to participate in the PoS system. On 05/21/19 there was 447.5 million XTZ delegated of a total 564.5 million XTZ staked - around 85% of XTZ participates in baking and 79% of that is delegated. Holders of XTZ can indirectly influence the governance of the chain by choosing which bakers to empower with their delegation, but it remains to be seen how actively holders will use this power and to what extent their decisions will be based on the pursuit of rewards. Delegation allows one to generate returns passively, and it is possible some delegators will pay little attention to their baker as long as the rewards keep coming.

Within the bakers constituency there are rules about baking and mechanisms for enforcement. Bakers are not allowed to double bake (bake on two forks of the Tezos chain) or endorse blocks on two chains. If they are caught doing so they forfeit their security deposit, with 50% of this going to the baker who accused them of breaking the rules. These rules are intended to solve the "nothing at stake" problem which could prevent a PoS system from converging around a single chain.

The Tezos Foundation controls the proceeds of the Tezos ICO (worth approximately $232 million at the time) and 10% of the initial XTZ tokens, and has a mandate to use these to give "support to Tezos and related technologies as well as to the Tezos community".

Bakers and holders have no say in how these ICO funds are used. The initial supply was composed of 607 million XTZ for ICO funders and 76 million XTZ for each of the Tezos Foundation and Dynamic Ledger Solutions (DLS) - for a total initial supply of 763 million XTZ. DLS is a company created by Arthur Breitman in 2015 to hold the rights to Tezos software, and contracted by the Tezos Foundation following the ICO to relinquish those rights and associated IP. Stakes in DLS were sold to early investors to raise funds for Tezos before the ICO.

A report published in Aug 2019 provides some insight into how the Tezos Foundation is managing its funds. They hold 61% of their $650 million USD equivalent as BTC, 15% as bonds/etfs/commodities, 15% as XTZ (their ICO tokens and staking rewards, untouched), 6% fiat. The Foundation funds a large number of initiatives but keeps the details of these arrangements (amounts, terms) private.

Tezos also has ongoing inflation, with ~42 million XTZ awarded to Bakers each year (or a target of ~5.5% annual inflation). 96% of the current total supply was issued to ICO participants. Given that many of those same ICO participants have elected the bakers and continued to collect a share of the inflation rewards, the outlook for Tezos is still closely tied to that initial set of participants and the decision-makers at the Foundation.

Protocol upgrades can include the creation of new XTZ tokens from inflation. The first Tezos mainnet upgrade included 100 XTZ tokens so that the developers who produced it could buy a round of drinks, so this mechanism is not playing

a significant role in funding Tezos development yet. This kind of funding will be limited to supporting entities that work on the protocol, as contributors to other aspects will not be in a position to bundle inflation XTZ with on chain proposals.

Arthur Breitman has recently written about a design for a simple on chain treasury, which if implemented will extend the influence stakeholders have over the direction development takes.

Decred

Decred uses a hybrid PoW/PoS method of reaching consensus, PoW miners perform the same basic function as in Bitcoin but the network's rules are designed to give PoS voters power over the miners. Holders of DCR (Decred's native asset) can time-lock it in exchange for tickets, and voting with these tickets is how Decred makes decisions about the consensus rules of the network and how development should be funded.

In short, Decred 1) carefully defines a constituency of stakeholders that have collective responsibility for governing the network, and 2) embeds mechanisms through which this constituency of stakeholders can make and implement decisions. The stakeholder constituency is defined as people who are willing to time-lock their DCR until their ticket is called (up to 4 months), with the rationale that these people have skin in the game and are incentivized to look out for the network's best interests.

Various stakeholder groups (miners, users, developers) comingle in this unitary stakeholder constituency, and have decision-making power commensurate with the amount they have at stake. This simplifies governance, as compared to a project where the various stakeholder groups have different affordances in how they can exert power over the project (sometimes resulting in an impasse or fracturing of the ecosystem).

Consensus PoW miners compete to solve random puzzles and create new blocks, providing security for the network and collecting 60% of the block reward and all transaction fees. PoS voters are pseudorandomly called to vote in each block, and the blocks are not recognized as valid by the network until at least 3 (of 5) tickets called have voted. Tickets vote to approve or reject the contents of the previous block, giving them the power to reject a miner's block for a specific reason and withhold that miner's reward, without interfering with their own reward.

The requirement that each block have the active participation of at least 3 (of 5) randomly selected tickets makes the network significantly more robust to majority attacks. This is because selfish/secret mining is impractical without controlling a significant share of the live tickets and ticket voters will not vote on blocks that would result in a significant reorg. In effect, PoW and PoS constitute

a two-factor approach to security, where an attacker must compromise both factors to succeed. PoS voters receive 30% of the block reward in exchange for the service they provide in improving the network's security and participating in governance.

The requirement that each block be shown to ticket-holder constituency before it can be completed and broadcast means that the blockchain must be constructed, *block by block*, on the commons. This is in contrast to pure PoW blockchains, where a competing chain can be worked on in private and then released on the network whenever its miners choose. The nodes willingly accept this alternative chain as long as it has more accumulated PoW, even if it rewrites their version of the chain.

Decred tickets are also part of a formal decentralized method of approving and adopting changes to the consensus rules. To trigger this process the nodes run by PoW miners (95%) and PoS voters (75%) must upgrade their software to a new version which incorporates a latent set of changes to the rules. For a period of ~28 days every ticket that is called can vote to approve or reject the proposed changes, if at least 75% of voting tickets approve the changes then they are activated 28 days later. This means of coordination ensures that Decred can deploy hard fork upgrades smoothly in the case where they are supported by ticket-voting stakeholders.

Funding Development of the Decred project is funded by a Treasury which receives 10% of the block rewards. Ticket holders vote to approve or reject proposals for how those funds should be spent, and these decisions are implemented by paid contractors. An LLC entity called the Decred Holdings Group is in charge of making the payments from the Treasury wallet. Decred plans to subject monthly spending to a ticket vote, giving the ticket-voting collective ultimate authority over this aspect of the project as well.

Decred's funding model can be understood as an attempt to merge conventional approaches to FOSS development with an autonomous funding source and the broader objective of building a robust network. To isolate the weakness of centralization, the project seeks ways to entrust a decentralized collective with overseeing the development of the network, making decisions about the common pool resource itself and how the available funds should be used to improve it.

The degree of control that stake-voters exert over this Treasury is deliberately loose, confined to signalling approval or rejection of proposed spending (and in the future approving each aggregated monthly spend). Specifically, proposals which are intended to dictate how contributors (e.g. wallet developers) approach their work are not allowed.

This approach is intended to preserve the autonomy of contributors and create a good working environment and inventive structure. From the intrinsic/extrinsic motivation perspective, Decred's approach seems to strike a good balance between the autonomy of contributors and the need to maintain cohesion within the

project's funded work. Extrinsic rewards (payment) are available but the degree of control exerted over contributors is minimized. Stakeholders control this at a strategic level by voting to approve or reject programs of work and their associated budgets.

Paid contributors to Decred are referred to as contractors, and contractors can be either individuals or corporations (which employ a group of contributors). Contractors submit monthly invoices to be paid for their work.

On the surface this appears as production which is coordinated through contracting with external parties, but in practice the "contractor collective" exhibits some of the same characteristics as a firm with employees. New members are invited to join when they have contributed work to some of the funded projects and the other contributors to those projects find their work to be of an appropriate standard. The conventional approach of receiving applications and conducting interviews is eschewed in favour of demonstrated ability to make valued contributions.

There are plans for a clearance process whereby a new contributor must be approved by established contributors in their domain before they can start billing for their work. Those other contributors within a domain will also have the power to revoke a contractor's clearance - with a method of escalating disputes to a vote of all contractors, and from there to a stakeholder vote if necessary. The intention is to allow groups working on specific aspects to function independently without hierarchical control from outside the group; while maintaining a degree of oversight and accountability which is needed to ensure that sub-projects stay on target and Treasury funds are not wasted.

Decred's approach to managing its block reward Treasury is uniquely tailored to the FOSS context. Some of its founders and lead developers have experience of working on FOSS projects pre-blockchain, and on an independent implementation of a Bitcoin full node, and have witnessed the tragedy of the commons firsthand. Decred's funding mechanism has been developed to address a specific need, and the way it is administered is designed to minimize the friction with how FOSS projects operate. The great majority of these funds are used to incentivize contributors to the various FOSS projects that make up the Decred ecosystem, and the open source ethos runs deep within the project.

Almost all of this work and the coordination around it happens on the commons, and Decred strives to create FOSS tools that offer new types of commons which facilitate this coordination. Politeia is a good example of this. It is an off chain governance platform (modelled on reddit) where proposals can be submitted and discussed in an environment with accountable censorship, where an immutable record of proceedings is maintained. Politeia uses dcrtime software to anchor its data to the Decred blockchain every hour, ensuring that the administrators of the server cannot secretly distort its contents or censor particular points of view.

Politeia Politeia was developed because it was deemed necessary to allow for censorship of proposals and comments on the open governance platform - otherwise it would be vulnerable to spam and illegal content. The requirement of being able to censor inappropriate content necessitates administrators who can wield this power.

Ultimately, whoever runs the server that hosts a service has the power to inspect and edit its data/content. In the context of the governance of a decentralized project like Decred, this kind of power could be abused to pursue the administrators' agenda. For example, by censoring proposals or comments that advocate for a course of action they deem undesirable, marginalizing members of the community who hold those views.

Politeia users get "censorship tokens" which they can use to prove that they submitted a particular proposal, in the event that it is censored by an administrator without public acknowledgement. There is also a small cost (~2$) associated with submitting a proposal (to prevent spam), and with creating a Politeia account - to make it more difficult to make multiple accounts to spam the platform or spoof support for some point of view.

The Politeia software is FOSS, with a specific instance being used to host Decred proposal discussion and show ticket voting outcomes. As the software is FOSS, there is no barrier to another group hosting a new instance in the case where the instance hosted by Company 0 developed some problem.

Company 0 is the organization that produced btcd and was a major force behind bringing Decred into being. In the early days, Company 0, an organization employing a number of the most active developers, was a dominant influence on the project. Over time their influence and share of Treasury spending is waning.

The data for public proposals and comments and up/down votes on comments is all available through a GitHub repository, allowing anyone to verify that the data is unchanged by using it to check that it matches what was anchored in the Decred blockchain. The presence of up/down voting functionality means that were these votes to be anonymous (as they are on reddit) only the administrators would be able to inspect them and selectively reveal them (e.g. to identify or accuse of sockpuppet voting). Politeia tracks these votes openly in the data repository, with the idea again being to make this commons as fair as possible for everyone who uses it to participate in Decred's governance.

Politeia also serves as the basis for a Contractor Management System, which is used to collect, record and process the monthly invoices from contractors. This information too is recorded immutably (although not publicly readable), so that members are assured that the information they can access is uncorrupted. Invoices are cryptographically signed by their submitter and anchored in the Decred chain, there is no way to edit or delete them. Public aggregated spending summaries are also planned, and these will benefit from the same assurances.

Decred's Treasury funds are used to further the project in ways other than

software development, in recognition of the fact that the project is about building a useful public common pool resource. The nature of cryptocurrencies is that they get more useful the more people use them (network effects), and so promoting use of the Decred network is integral to this resource's value. Work towards this goal is funded by the Treasury. In practice the stakeholders decide what the scope of the project is, both directly (by, for example, amending the project's constitution) and indirectly by deciding which work should be funded. One of the most controversial decisions so far has been about whether to hire a specific PR firm (Ditto proposal), the proposal was approved and the firm's position renewed for 6 months later with another proposal.

As noted above, this resource is itself also partially funded by the Decred Treasury, as part of an Open Source Research program (also recently renewed). This research program processes and analyses data from Politeia to produce insights about the platform that can be shared back with the ecosystem. It also looks beyond Decred to see how other projects are approaching the aim of decentralization, where there are successes and failures. Decred is actively working to inform its stakeholders and improve their collective intelligence, in the expectation that an engaged, informed and cohesive stakeholder constituency is where the network's strength will be derived.

Membership of the stakeholder constituency is permissionless, it only requires enough DCR for a ticket (at time of writing in June 2019, around $3,500), and voting power is decentralized to a large and growing degree (see Distribution section below). All software and information goods are offered openly on the commons as public resources, ensuring that they are available to all stakeholders, and external observers (who could become stakeholders at any point).

Governance The salient points about Decred's governance are these:

- PoS ticket-voters contribute to block validation in a way which gives them authority over PoW miners
- ticket-holders vote to accept or reject changes to the consensus rules, on chain.
- ticket-holders vote to accept or reject budget and policy proposals, on Politeia.
- participation on Politeia through comments and reddit-style up/down comment votes is open to anyone that pays the 0.1 DCR (~$2) registration fee. Proposals cost 0.1 DCR each.
- work is coordinated through (almost universally public) Github Repositories and chat rooms (bridged between Slack, Discord and Matrix). These chat rooms also play a role in governance, as they are where participants hold informal discussions about the issues at hand. I wrote up this analogy about how the various social platforms fit together.

Stake-voters are integral to producing the blockchain but they do not directly drive the project, rather they open and close gates with decisions about the

consensus rules and Treasury spending. The contractors working directly on the project have a different kind of influence on its progress and direction. Workers are in the first instance accountable to their peers, but as groups they are ultimately accountable to the decentralized stake-voter constituency. This can be thought of as a kind of informal delegation, but more a delegation of work than decision-making power.

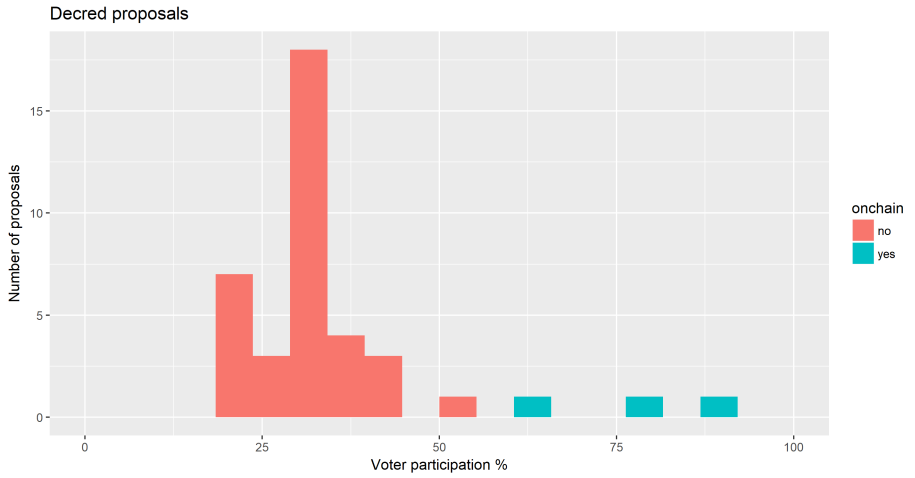
Formal delegation is isolated to "Voting Service Providers" (VSPs). A VSP is a service that will vote on a stakeholder's behalf when their ticket is called to vote on chain. When a ticket is called to vote it must respond quickly, and this means a wallet must be online and open at that time. When stakeholders buy tickets they can allow a VSP to vote on their behalf, thus delegating some of their sovereignty (but not custody of their funds) in exchange for the convenience of not having to continuously maintain open voting wallets on their own servers. Stakeholders decide how they wish their tickets to vote on any open consensus rule change proposals, and the VSP is responsible for voting in accordance with that expressed wish when the time comes (stakeholders can easily check how their tickets voted). Politeia voting is not delegated in any way, the holder of the ticket votes directly from their wallet.

Politeia has a limited role for administrators, who are charged with censoring spam and inappropriate proposals, and who control the start of voting periods.

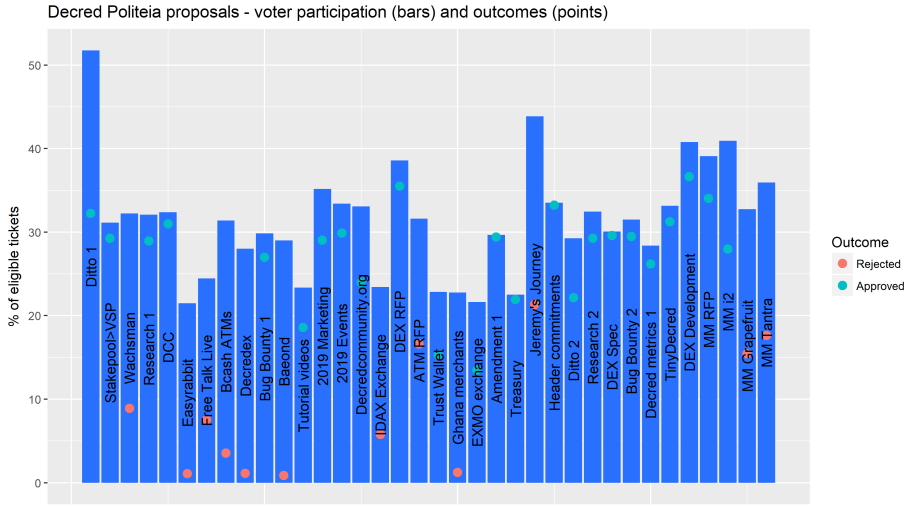
Politeia proposals that pass this review process are published for discussion, and can be edited by their owner as the discussion unfolds (with the platform maintaining a history of previous versions). When the discussion has reached a conclusion the proposal owner authorizes the start of voting and an admin triggers this week-long voting period. The proposal must be voted on by at least 20% of eligible tickets, and receive at least 60% Yes votes to be approved.

Participation in Decred's governance is relatively high, with around 50% of circulating DCR being time-locked in exchange for tickets at any given time circa mid-2019. Politeia launched in October 2018, and as of September 14 2019:

- There have been 4 on chain consensus rule change proposals with mean active ticket participation (i.e. voting yes or no) of 69%. All of these have had near unanimous support as they represented uncontroversial protocol upgrades. One change may have proven controversial with miners if they had veto power within the system because it reduced the fees associated with ticket transactions.
- There have been 36 Politeia proposals which have made it to a vote, with mean ticket participation in those votes of 31.5%. An additional 14 proposals have been abandoned or are still under discussion.



24 proposals have been approved and 12 rejected. Proposals have been approved which cover decisions like hiring a PR firm, approving a marketing budget, various research projects, DEX infrastructure, Python tools, a bug bounty, and policy decisions like a new contractor clearance process and an amendment of the project's constitution.



Once proposals are approved, the contractor collective is responsible for ensuring that the work is completed satisfactorily, at which point the workers can invoice against the approved budget and be paid.

Distribution It is not possible to know how many different people are represented among the Decred ticket-voters, but we can make some inferences by considering how DCR has been distributed.

Decred began with an premine and airdrop (description reproduced from previous section). 4% of the 21 million DCR total supply was allocated to the founders and another 4% airdropped for free to 2,972 participants who signed up following an announcement in the bitcointalk forum and picked up on Slashdot. In Decred's case some form of premine was necessary to distribute DCR so that a decentralized set of users could buy tickets to power the PoS system. After a period of around 15 days (4,096 blocks) of pure PoW (in which time holders could get set up to vote) the PoS system automatically activated. Without a premine the early PoW miners would have dominated PoS as they would have been the only entities with DCR to stake.

In June 2019 after more than 3 years in production, 10 million DCR had been created, of which 1.68 million were issued in the genesis airdrop, PoW miners had received 5 million DCR (~50%), PoS voters had received 2.5 million DCR (~25%) and the Treasury had received 830k DCR (~8%). PoW miners typically have strong sell pressure to meet their operational costs and so it is likely that a significant fraction of the DCR they mined has been sold to cover costs. PoS voting rewards will have gone to people who received the airdrop, mined DCR or bought it on the market - then locked their DCR to buy tickets. Importantly, the proportion of new DCR going to PoS voters is low enough that they cannot maintain their share of the growing issuance or their representation in governance (number of tickets) just by staking.

Dash

Consensus Dash uses PoW consensus with a special role for "master nodes" that have collateral of 1000 DASH (at time of writing in June 2019, around $163,000), this model is referred to as "Proof of Service" (PoSe), or more commonly by reference to masternodes (there are many projects which have emulated the master node concept). This is conceptually similar to Proof of Stake, in that master nodes must demonstrate that they have something at stake in order to participate. Master nodes must also continuously run a node on a server which meets certain minimum requirements. The network's InstantSend and PrivateSend features are provided through master nodes. Dash also recently added " ChainLocks" which are checkpoints constructed by a set of master nodes that make double spend attacks harder to execute without controlling a significant proportion of master nodes. Dash does not require master node collateral to be "staked", meaning that a master node owner can liquidate their collateral at any point.

Once a quorum of masternodes attest to having seen the same new valid block, they sign a transaction that locks it in and would reject any chain which does not have this block. This gives master node owners the power to prevent miners from executing a reorg, which is significant, but it does not give them any scope to reject other forms of misbehavior by miners.

The Dash PoW miner and master node constituencies both receive 45% of the block rewards (miners also receive transaction fees), with the remaining 10% being distributed through a Treasury DAO.

Like Decred, Dash is based on the principle that the master node operators are the key decision-making constituency, but the specific mechanisms through which master nodes make and implement their decisions are quite different.

Funding Dash's commons-based governance is focused on the distribution of Treasury funds, which follows a formal on chain decision-making process. Every 16,616 blocks (approx. 30.29 days) a "superblock" is created which spends that month's accumulated Treasury stipend.

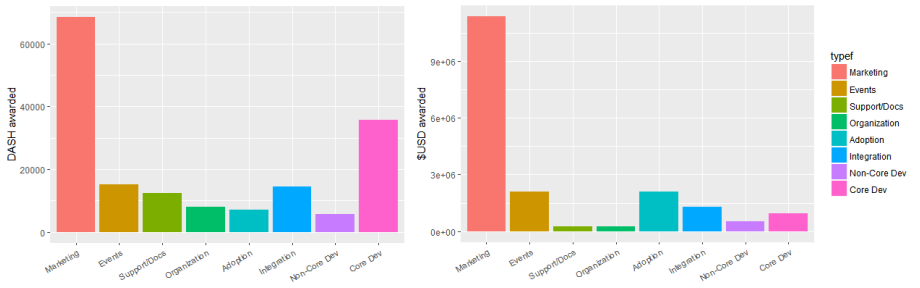
Proposals are submitted on chain by people who offer to perform certain services. Making a proposal is permissionless, although a fee of 5 DASH (~$800) is an effective spam deterrent. This fee is not returned unless the proposal is approved, so it also discourages the submission of relatively small scale proposals or proposals from people who do not have this kind of DASH to spare.

Master nodes vote Yes or No on these proposals, and at the designated time the votes are tallied. The proposals are ranked and an eligibility criteria applied (a Yes - No score of greater than 10% of eligible master nodes). The available funds are paid out to the top scoring proposals. Where there are not enough funds to pay all eligible proposals, the lowest scoring proposals are not paid. In effect the proposals compete directly with the cohort of other proposals up for consideration in the same month. This means that the timing of a proposal is important, determining the strength of the competition it faces.

Where there are not enough eligible proposals to account for all the available DASH, the surplus amount is not created. The Dash Treasury has no capacity to save.

The actual content of the proposals would bloat the chain, and so these are stored off chain in bespoke platforms like Dash Central. Such platforms facilitate commenting but there are rarely substantive discussions in their comments. If significant deliberation about proposals happens on the Dash commons, I have yet to identify where. The project's Discord chat rooms are a possible venue for this, but from the limited time I have spent observing them it did not seem like there was much substantive discussion of proposals.

I studied Dash's Treasury DAO and published a couple of articles about it in 2018. The first about how it had been going and what it was being used to fund. The second about the various support structures surrounding it, and what Decred could learn from these ahead of Politeia's launch.



DASH is unique in that it has been controlling distribution of funds in a decentralized manner for a number of years already, and its Treasury has already spent a lot of DASH in this way. This makes it possible to assess how the master node voting system has been behaving, to consider whether it has been making good decisions about how to spend available resources and how well that process is going.

To summarize the linked articles, the Dash DAO is conceptually interesting but it seems like the rigid and basic on chain process for distributing funds presents some obstacles that must be worked around. The master node voting makes the process as decentralized as the distribution of master nodes, but this comes with significant trade-offs. The rapid expansion of highly speculative advertising, promotion and marketing proposal budgets during the bull market of 2017 is a good example of the limitations of the system.

Governance On the surface, Dash tends towards the ideal of a nexus of contracts instead of a firm with employees. In this case the contracts are embedded in the Dash protocol and signed/enacted by the decentralized master node collective. The protocol makes payments up front as soon as proposals are approved, omitting the transaction costs associated with ensuring that the contracts are followed through but leaving the Treasury open to exploitation as a result. Trusted escrow providers have stepped in to fill this void, acting as an intermediary between the DAO and the contractor, holding the Treasury's DASH until they confirm that requirements are met, and charging a fee for this service. More recently, the services of Dash Watch have been retained to liaise with proposal owners and report on their progress.

At the core of Dash's Treasury spending is a long-standing relationship with Dash Core Group Inc, which has been a recipient of Treasury funds since the beginning. The master node collective has effectively delegated a large part of their decision-making power to Dash Core Group, a conventionally run corporation with quite a few employees. Dash Core Group has autonomy to develop the project's core software, and change the network's consensus rules, in whatever way they perceive as best. The master nodes indirectly control DCG through control of its funding, and they have always had the power to withdraw this. In 2018 a legal entity was created through which the Dash master node DAO could legally own and control DCG, and some mechanisms were put in place whereby the

DAO could steer DCG.

In characterizing the Dash commons, the presence of this monolithic corporate entity is no doubt significant, as this is where key decisions about the project's future (e.g. ChainLocks and "Dash Evolution") are made. DCG is also the entity responsible for delivering on these decisions. The mechanism for deploying hard fork upgrades is similar to Bitcoin, in that the Core group releases software which has an activation rule depending on miner and master node adoption, once these criteria are met the change activates. Much of Dash's governance happens in the interplay between DCG and the master node collective, but in practice this has so far been limited to a few signalling proposals, with very few occasions where the master nodes challenged DCG.

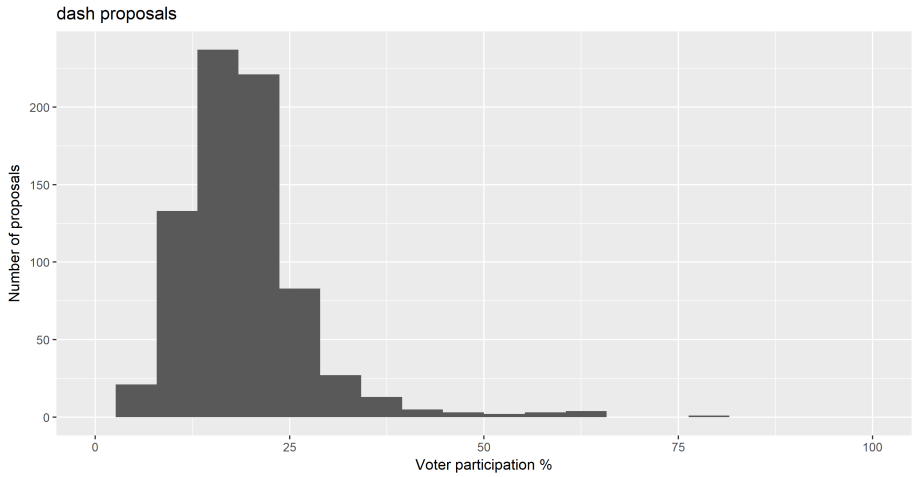
Dash has historically spent a significant proportion of its Treasury funding on marketing and promotion, although this was drastically reduced over the course of the 2018 bear market.

More recently, DCG has established Dash Investment Foundation, which will allow the Dash project to invest in projects and receive equity in exchange. An election in which master nodes choose board representatives for this foundation recently concluded, and it will be followed by on chain proposals which allocate DASH to be used as capital by the foundation. This will give the project (in practice the people running this foundation) a way to further shape the Dash ecosystem and own pieces of it.

The ways in which the crypto commons interface with legal and regulatory constructs is itself an interesting subject to study, and Dash has certainly devoted some effort to giving its master node operated DAO legal standing.

There are presently around 4,500 Dash master nodes, although it is not known how many individuals operate clusters of these nodes, the number of individual people involved is likely considerably fewer.

For the first 758 Treasury proposals (August 2015 - April 2019) mean master node participation in voting was around 19%.



Dash does not have an accessible website which showcases all of its historical proposals and their voting outcomes. I used Dashvotetracker for this until it was abandoned by its maintainer. Now the master node community seems to use Dash Nexus for the purpose of tracking proposal voting. It does a good job of presenting the live proposal voting status but offers very limited historical data. Dash Nexus also has a space for "Concepts", which seems to function similarly to the "pre-proposals" discussion board, where people can explain their proposal and seek feedback before committing the $800 proposal fee.

Distribution There is a controversy in Dash's history around an "instamine bug" which allowed large quantities of DASH to be mined in the first days of the network - likely mined largely by the developers. There are many relevant sources for this, here are two that represent each side:

- bitcointalk post from 2015 where the launch was discussed in detail
- "official reponse" to the instamine from Dash Core Group

All parties agree that: much more DASH was mined in the first 48 hours after the chain launched than was intended - 2 million DASH were minted during this time, around 10% of the total supply that will ever be issued. Dash proponents argue that participants consented to forging ahead with the chain despite the flawed start, and to a subsequent decrease in the maximum supply, and that a large proportion of the instamined Dash was traded on the market at a low price. Dash detractors argue that the launch was deeply flawed, that there is no way to know how much DASH the founders mined and retained, and that 45% of the block reward would allow them to retain their relative influence and share of the DASH at low cost by operating master nodes.

Zcash

Zcash relies on pure PoW consensus and is mined by ASICs. Having formerly considered itself "ASIC resistant", it made no moves to interfere with the deployment of ASICs on the network and now takes a neutral position towards them.

Zcash's commons are dominated by two conventional organizations, the Electric Coin Company (ECC) and the Zcash Foundation. Zcash uses pure PoW consensus but incorporates a "founder's reward" through which 20% of block rewards are issued to the founders - stakeholders in the Zcash company (now "Electric Coin Company" or ECC).

The ECC (formerly Zcash ECC) took investment before launching Zcash, and the founder's reward is distributed between founders, investors, employees, and advisors according to some private contractual arrangements. Zcash is pioneering the use of zero-knowledge proofs to allow for private transactions, and the founder's reward is predicated on the idea that the developers are highly skilled and they can only dedicate much of their time to working on the project if they are well compensated.

> How can such a high-powered team afford to devote years of our lives to this project when everything we're producing is public, open, and permissionless?
>
> Zooko Wilcox

As the focus is on cutting edge cryptography and Zcash is a work in progress, it can be assumed that Zcash ecosystem participants are comfortable with accepting hard fork upgrades as and when they are released by the ECC.

Zcash launched in October 2016. Five months later Zooko announced the Zcash Foundation.

> The organization we created to launch this project is a startup. This provides a tight-knit, focused team, rapid decision-making, and the possibility of generating additional funding, such as by building blockchain solutions for industry.
>
> However in the long run it would not be appropriate for a single for-profit company to have this much power over the evolution of the Zcash technology. Ultimately, there will need to be an independent, inclusive, non-profit body to steward the technology in the interests of all users.
>
> - Zooko Wilcox

Zooko and other ECC members donated portions of their share of the Founders' Reward totalling 273K ZEC, at then price of $49/ZEC it was worth $13 million+.

> I personally have donated half of all of the coins I was due to get from the Founders' Reward, and many of my colleagues have donated as generously or even more so!
>
> - Zooko Wilcox

The Founder's reward is 10% of the total ZEC issuance, 2.1 million ZEC - so the Zcash foundation is set to receive 13% of the Founder's Reward in total, over the first four years of the project. When the first halving in block rewards occurs after roughly four years, the Founder's Reward is set to cease, which would cut funding to ECC and the Foundation. All block rewards would go to PoW miners from then on, according to the current consensus rules.

The attention of the Zcash ecosystem has recently turned towards sustaining development beyond the duration of the founders' reward, with Zooko expressing support for a continuation of block reward funding which incorporated ECC but had a larger role for other organizations. In his capacity as ECC CEO, Zooko has stated that the ECC needs 12 months of runway to function and if no continuation of funding for ECC is established one year before the founder's reward ends, then ECC will have to consider pivoting to other projects which can generate revenue.

The scenario is familiar to other projects whose commons are dominated by a conventional organization. The many ICO funded projects out there received one-time funding, but what they are building will need perpetual maintenance and possibly refinement, if it succeeds. The Zcash funding issue is therefore of particular interest, because it is on the horizon for many other projects with autonomous but time-limited funding.

Organizations will tend to prioritize their own survival, and in many cases the continued vitality of the common pool resource would seem to depend on this dominant organization's continued leadership. Some of the ICOs took in significant sums which, if managed well could sustain development for some time. There are indications that ICO beneficiaries may not always be acting prudently with these funds.

That is not to suggest that the Zcash Founder's Reward is being mismanaged. According to this tweet, as of June 2018 the Zcash Co (now ECC) had a burn rate of $500k/month and 26 employees, this would be around $19k per person per month.

As the main leadership figure in the ZEC ecosystem, Zooko has had a challenging time navigating this issue of the funding gap post-2020. He has repeatedly stated that the decision of how to fund development post-halvening should not be taken by himself, and that the ECC should not be dictating what the next steps are because it is potentially a main beneficiary.

The Zcash community have been forthcoming with many suggestions. Chris Burniske of Placeholder VC, a recent investor in ZEC, made a detailed analysis of the situation. This advocated for a continuation of 20% block reward to

fund project development for another 4 years, with a split of 70% to "Protocol Development" and 30% to "Growth Funds", while recognizing that there were other options on the table (like a drop to 10% development subsidy).

Burniske also highlighted the need to establish that the method of decision-making is seen as legitimate by all stakeholders in the Zcash ecosystem.

As Zcash is a commons-based resource, there is a risk of contentious fork if a significant faction within the ecosystem is not on board with the change that is offered by ECC. As this is a proposal to change the consensus rules, it can only be implemented and "offered" to the ecosystem by developers.

This saga has already led to a "friendly fork" called Ycash, which is independent of the ECC and Zcash Foundation and hard forked in July 2019 to reduce the Founder's Reward immediately to a perpetual 5% (now directed to the Ycash Foundation) - thus limiting development funding to 10% of total issuance as initially agreed. Ycash also plans to amend the hashing algorithm to pursue ASIC resistance. The development plan for Ycash is to track and incorporate most upstream changes from Zcash. Zooko wrote a blog post about "A Future Friendly Fork" in 2017, and this appears to have inspired the positioning of Ycash as a friendly fork. Zooko has also commented on the Ycash post to say that he sees Ycash as a positive development for Zcash.

It is worth noting that Zcash ecosystem constituents are no longer entirely reliant on ECC for Zcash node software. The Parity team released a Rust implementation of the Zcash protocol, sponsored by the Zcash Foundation. This reduces reliance on the ECC, and adds a degree of redundancy to enforcement of the consensus rules - where one version may be robust to an exploitable weakness in the other version and could serve to raise the alarm that something was amiss.

The ECC is in many ways the official custodian of the Zcash network, bearing great responsibility for the health of the network, and having significant power to amend the rules. One story from Zcash's history is particularly interesting in this regard. In February 2019, a team of ECC developers announced that they had identified (11 months previously), and stealthily deployed a fix for, a vulnerability in the underlying cryptography Zcash uses for shielded transactions. If exploited, this would have allowed an attacker to mint new ZEC without being detected. There is no way to know if this exploit was used. The way zero-knowledge proofs are deployed means that it is not possible to audit the full ZEC supply and ensure that it is as expected.

The blog post announcing the fix offered consolation in the likelihood that because this was such a complex exploit to identify only the highly skilled and expert members of the ECC team were likely to have identified it. From this perspective, giving developers with the deepest knowledge of the protocol a financial stake in it is probably a good use of block rewards to pay for security. If the individual who discovered the exploit first was not being rewarded with a steady supply of ZEC, they may have been more likely to consider stealthily minting some ZEC for themselves.

The severity of the threat to ZEC led the ECC members to keep it quiet for 11 months while they sneaked in a change to the consensus rules which would nullify the exploit, into a scheduled hard fork update. ECC was in this case withholding information from the Zcash stakeholders for their own benefit. The fact that nobody outside of the small group identified this change to the consensus rules before it was deployed and announced says something about the degree to which the Zcash commons are entrusted to ECC.

The Zcash Foundation has a mandate to represent the Zcash stakeholder community, and ample funding. This blog post from 2018 gives some insight into how the foundation is going about ascertaining the desires of the Zcash stakeholders. Their approach involves selecting up to 200 members of the Zcash community to form a Community Governance Panel. 64 initial CGP participants voted on a number of ballots at a foundation conference (including a rejection of ASIC resistance), and elected two board representatives to fill vacant seats on the Foundation's board.

The role of the CGP is effectively to inform the positioning of the Foundation, which itself has limited say in the future direction of the Zcash network. This page was updated recently (Q3 2019) to provide some resources related to the dev fund issue - a set of documents which provide summaries and make recommendations. Among these, the ZF has taken a position that any future mandatory development funding from block rewards should only be distributed to not-for-profit entities. The ECC is a for-profit corporation, ZF suggest that the obligation of this corporation to its shareholders represents a significant conflict of interest with the health of the network. ZF is taking the position that ECC should become a not-for-profit.

Another issue identified in the early part of this resource has more recently come into play with regard to the Zcash dev fund: ownership of intellectual property such as trademarks. There had been a long-standing agreement in principle between ECC and ZF that control of the trademark should be shared between these entities in the legal equivalent of a "2-of-2 multisig" but in Aug 2019 it seems that negotiations on the specifics broke down. Zooko posted about this disagreement:

> There are a few things that we've learned about the disadvantages of the 2-of-2 "double-veto" approach. One is the inherent problem with double-veto, which has been illuminated as we worked on the legal agreement and received 3rd party feedback. The inherent problem with double-veto is that it is prone to inaction or deadlock. Our earlier intention had been that 2-of-2 would be a stepping stone to 2-of-3, or even further decentralization. But, if we were to lock the trademark into a 2-of-2 double veto, and then there wasn't subsequent agreement on how to further decentralize it, then it would be in a dead end. There would be no way to move on to 2-of-3 or another more decentralized governance structure.

ZF is not happy about this development, stating that their position was very different, and that the news that the 2-of-2 multisig would not happen came as a surprise to them. ZF and other contributors to the debate are now suggesting that control of the trademark must be resolved before deliberation on the development fund can proceed.

Zcash's issues with development funding are a contemporary demonstration of the importance of governance for cryptocurrency networks. At the point where a formal governance process would help to resolve a dispute it can be too late to add one. Forging ahead with "rough consensus" and adding in a new governance process both run the risk of alienating some of the blockchain's constituents.

DAOs

The concept of a Decentralized Autonomous Organization (DAO) describes an organization which conducts aspects of its decision-making and the execution of those decisions on the crypto commons. A DAO that is effectively decentralized should limit the degree to which the organization relies on specific individuals arranged in a hierarchy, and could derive robustness to various forms of attack from this.

Blockchains excel at imposing rules on participants' actions, they are excellent bureaucracies. The flexibility of software means that it is possible to encode a wide variety of interaction types within a system. A DAO can embed some of its organizing principles in code and ensure that they will be upheld by all participants in a way which is robust and efficient.

The Decred and Dash projects described above have a form of DAO which governs certain aspects of the network and its development. In Dash's case the method of selecting and funding proposals functions as a basic DAO. In Decred's case the stakeholder DAO oversees the network and changes to consensus rules, while also signalling which programs of work the collective of contractors should be funded to work on.

Other projects strive to build general purpose DAO infrastructure that lives on a blockchain (usually Ethereum's) and derives its reliability from this blockchain - but is intended to be useful in a variety of contexts to DAOs with different purposes.

Network DAOs exist because there is need for a decentralized way of governing and distributing resources in a particular context. DAO platforms exist because there are people who believe DAOs can be much more broadly useful as ways to facilitate trust-minimized coordination. In the absence of examples that demonstrate the productive use of DAOs for a variety of purposes, DAO platforms all implicitly have the task of seeking out productive use cases. Their success depends on identifying these use cases and serving them well. This contrasts with network DAOs, which are engineered to serve a purpose within an existing

endeavour (running a blockchain).

There follow short profiles of some of the better known DAO platforms and a look at an example of one of the most significant DAO instances which uses it.

Aragon

Aragon is a platform for creating organizations that are "digital natives", it is concerned as much with building a digital jurisdiction for these organizations as it is with facilitating their creation. For now these DAOs live on the Ethereum blockchain as a set of voting-powered smart contracts through which the members of an organization make decisions (primarily about resource allocation) and have their collective decisions automatically actioned. Aragon pitches these organizations as "bureaucracy-free", but I think it is more accurate to describe them as having a highly efficient and automated bureaucracy. The toolset that Aragon currently offers is geared towards groups administering shared asset pools according to the outcomes of votes. Members deposit digital assets in a common pool and withdrawing or spending these assets requires a vote to pass. The DAO can mint its own tokens for voting and assign these to its members.

So far 570 DAOs have been created using Aragon on Ethereum's mainnet. It is difficult to get a sense of how many of these DAOs are being actively used, and of what they are being used for. Inspection of the tools available suggests that they would be suited to a members club that wished to make group decisions about how to allocate a shared pool of Ethereum tokens. Use of the Aragon platform gives these groups a way to allocate decision-making power among members (similar to voting shares) and then to create and vote on proposals with specified approval criteria (quorum and approval requirements).

Aragon makes it relatively easy to create these proposals, but presumably the bigger draw is in having a way to reliably conduct this kind of binding poll. There is some degree of trust minimization involved as well, but there is limited utility for this while most proposal outcomes are to simply transfer X tokens to some Ethereum address (owned by a party which can be trusted to follow through on the intended use for the tokens). Presumably in future the DAOs will be able to take other actions relating to smart contracts, and have a greater range of possible actions to take as the outcomes of proposals - but for now they look a little like amped up multi-sig wallets.

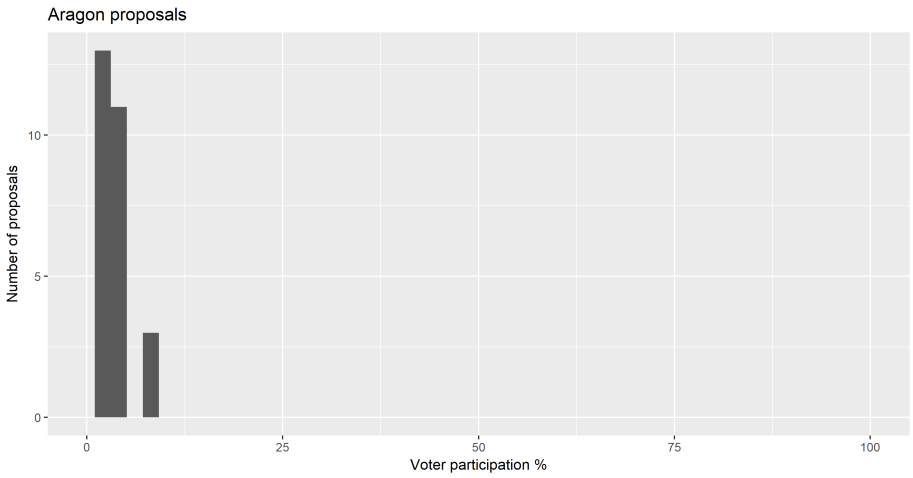
Aragon conducted an ICO in May 2017 in which they collected 275k ETH (worth ~$25 million at the time) over the course of 26 minutes, making it the second largest crowdfunding event in the blockchain space (after the DAO) at that time. 75% of the ANT tokens were distributed to ICO participants, 15% to the founders and early contributors (with a 2 year vesting schedule) and 15% to an Aragon Foundation. It seems likely that Aragon One took custody of the ICO contributions but this is not clearly documented. The post announcing the ICO stated that this would be the total supply until such times as an Aragon

network goes into production and sets its own "monetary policy".

The ANT tokens themselves are utility tokens which can be used to participate in dispute resolution processes in the Aragon Network, a "digital jurisdiction" which is yet to be released.

ANT tokens also confer voting rights in the Aragon Governance Proposals (AGP) process, through which ANT holders vote to decide which proposals to fund. Proposals are submitted through GitHub, and the Aragon Association decides which proposals are put forward for voting. Proposals typically request core funding in DAI (stablecoin) and some ANT on a vesting schedule as an incentive to improve the utility of Aragon and increase the value of ANT.

There have been three rounds of AGP voting thus far in which 27 proposals have been voted on. Participation of ANT tokens has ranged from 2-8% (mean 3.7%).



Aragon is exceptional as a project which collected ICO funds and is making decisions about how they should be spent in a decentralized way, allowing the token holders themselves to vote on these decisions. There are 3 independent developer teams working on different aspects of this DAO tooling and jurisdiction - Aragon One, Autark Labs and Aragon Black.

Aragon's ultimate objective is to build a new type of commons for DAOs to inhabit, and to provide a set of tools which allow these organizations to be easily created and deployed.

A blog post in Jun 2019 described Aragon Fundraising, due to launch in a few months.

> Aragon Fundraising will be a funding platform where people who have projects or organisations can issue tokens on the market and receive money to help them finance their project. This platform will be the materialization of an idea presented one year ago by Vitalik Buterin

> and known under the acronym of DAICO (Decentralized Autonomous Initial Coin Offering). The general idea behind this model is as follows : A Decentralized Autonomous Organization (DAO) issues tokens that give its owners privileges in the organization or rights on the production of the DAO.

It is interesting that Aragon is now aiming to address the misalignment of incentives endemic within conventional ICOs. The aim is to do this by replacing the organization that holds ICO proceeds with a DAO that is controlled by the people who provided those funds (and the other constituencies that receive tokens, typically including founders).

BlankDAO

> BlankDAO is a social organization with an aim to break blockchain barriers on the road of decentralization by relying on real people instead of miners. BlankDAO is Currently an Aragon DAO

BlankDAO is an Aragon DAO whose purpose seems to be orchestrating a crowdsale (their white paper links to a google doc) so that it can build out its own infrastructure. The idea that the current Aragon DAO form is just a crude initial iteration is common to many of these projects.

The BlankDAO on Aragon mainnet is one of the most active and decentralized looking DAOs using Aragon as of June 2019. It has 25 members (addresses that hold voting tokens) and a fairly skewed distribution whereby the top 5 holders have 50% of voting power. Since it launched in February, BlankDAO has processed around 100 proposals. Most of these are transfers of tokens (usually DAI) and minting tokens for new members, but there are also more unique proposals like whether to raise the price of "Blank tokens" in the crowd sale, whether to modify the permission of a smart contract, and whether to "Remove any signs related to Israel militia group from Blankdao services" (BlankDAO founders are Iranian). The proposals as represented on the DAO interface have no descriptions or discussions, so is likely that it is supported by some off chain discussion platform.

BlankDAO highlights the pervasiveness of token sales in the Ethereum ecosystem, it lives on the Ethereum blockchain (funded by token sale), within an Aragon DAO (funded by token sale), and is using this DAO to organize its own token sale. Despite what is a reasonable degree of decentralization relative to other Aragon DAOs, most proposals are approved by just one or two of the largest voting token holders and relate to transactions that are not intelligible to outsiders.

DAOstack

DAOstack pitches itself more directly as a platform and toolset for creating DAOs, "An operating system for collective intelligence".

> DAOSTACK POWERS DECENTRALIZED COMPANIES, FUNDS AND MARKETS TO MAKE FAST AND INNOVATIVE DECISIONS AT SCALE.

Allowing these DAOs to operate at scale is central to DAOstack's approach, the key point of which is the use of prediction markets to facilitate decision-making that represents the majority's perspective without requiring the majority to participate. They refer to this as Holographic Consensus.

Within a DAO, members are assigned voting tokens and the DAO can perform certain operations (like sending resources from a pool it controls) when proposals are approved by a majority of the voting tokens. Some DAOs also allow GEN tokens to be exchanged for reputation (voting power), e.g. dxDAO. Ordinarily proposals require a majority of all the voting power for approval and have a long voting period. GEN tokens (issued by DAOstack in an ICO) can be "staked" to predict the outcome and "boost" the proposal such that its voting period is shortened and only a relative majority is required for the proposal to be approved and implemented.

The rationale for this system is that DAOs cannot scale to many decisions involving many people if all of the people must participate in all of the decisions. GEN holders who predict/stake could in principle allow the DAOs to make decisions that reflect the majority opinion without having to involve a majority of participants. DAOs effectively pay for this service by offering rewards to GEN stakers. GEN stakers operate by learning what a DAO values and how it operates so that they can accurately predict the outcomes of proposals.

This is an interesting concept which addresses a legitimate issue for DAOs that wish to make decisions at a high degree of granularity. Information overload and the scarcity of stakeholder attention are significant issues for any DAO (or other form of direct democracy) that reaches a large scale. Low voter participation means that outcomes are more easily swayed by direct beneficiaries or others who have a vested interest. High voter turnout from a large scale decentralized entity with many members is difficult to achieve and maintain. Participation must also be thoughtful or is likely to result in poor decisions.

DAOstack is another example of a project which is oriented towards addressing issues of scale that are likely to arise in the long term. The first challenge for these projects is to reach a scale of participation where their solutions can be demonstrated and tested.

Unlike Aragon, DAOstack DAOs are created manually by the project team. People who wish to form one first initiate contact with the project team. This allows for greater flexibility in how these DAOs are configured, but the gatekeeping

results in a smaller total number of DAOs using DAOstack's Alchemy (11 in June 2019). DAOstack plans to allow for direct creation of DAOs by users in future.

Genesis Alpha

Genesis Alpha is a DAO created by the DAOstack team on the Ethereum mainnet. It serves as a testing ground, a showcase of DAOstack's functionality, and a way to govern the use of some of the project's resources. At time of writing (June 2019) it controls around $21,000 worth of ETH, GEN and DAI. There are 183 reputation holders, the most influential of which holds 2.4%, so voting power is reasonably well distributed among the participants. To become a member, people create proposals requesting Rep, usually introducing themselves and being approved.

Kyber Network

The **Kyber Network** has tested an Aragon DAO and is currently trialling DAOstack. This is a rare example of a project which started without any formal governance but has recognized a need for decentralized governance and is now going through a community consultation and experimentation process to find a DAO type solution. In the first experiment, an Aragon DAO was created in which KNC tokens (Kyber Network's native asset) could vote. The first proposal asked whether a Community Grant should be set up to be governed by the KyberDAO, 95% of voting power approved this decision but only 0.56% of circulating KNC tokens were represented, across 60 unique addresses, so a maximum of 60 people participated. This illustrates a problem with adding formal governance based on token voting to projects which did not have that as part of their foundation. It is difficult for these votes to establish legitimacy with low turnout, and without established legitimacy many holders will not take the trouble to vote. Ethereum carbon votes are a good example of this, although they can achieve reasonable turnout for controversial issues, people who have more at stake will be more incentivized to participate, and so the low overall representation means the results tend to be swayed by those who would be directly affected.

Other Ethereum DAOs

"The DAO" is still for many people a particular initiative that happened on the Ethereum network in 2016. It was mentioned previously in the context of the hard fork which occurred in the aftermath of its failure, to erase the damage it did.

This early attempt at a Decentralized Autonomous Organization almost destroyed

the entire Ethereum commons where it was constructed, and in the end split it asunder.

The DAO aimed to create a decentralized venture capital fund, similar to Coase's concept of production organized through a nexus of (smart) contracts. It is unfortunate that we never got to see whether the DAO would overcome the transaction costs associated with this method of organizing production, whether it would make good or bad decisions, and whether decentralization of its "directors" would help or hinder.

The DAO was phenomenally successful as a crowdfunding effort, holding 14% of all ETH in existence, worth more than $100 million. This is particularly impressive for such a novel approach which had never been tried before, and is testament to the degree of excitement and buzz that must have permeated the Ethereum community at its launch.

Before the DAO could achieve anything of consequence it was "hacked". Someone exploited a series of vulnerabilities in its smart contracts to "steal" ETH valued at around $50 million. The DAO had been configured with a 28 day waiting period before the funds could be withdrawn, and this gave the Ethereum community time to consider how it would respond.

Some Ethereum founders and developers were likely exposed to the DAO's losses personally, giving them an incentive to make an exception and set the network's rules aside to nullify it. To have such a large proportion of all ETH be stolen also would not bode well for the price of the asset in a scenario where the attacker dumped even a small portion of their stolen ETH on the market. The only entity that stood to benefit directly from the enforcement of the rules in this case was the hacker.

This open access book chapter by Quinn DuPont provides a detailed history and ethnography of the DAO and its aftermath. It draws a stark contrast between the way the DAO's governance was believed to function by participants and how it actually functioned in practice when under stress.

The Ethereum Foundation released new node software which defaulted to a hard fork upgrade that would undo the DAO. This was adopted by most but not all of the Ethereum ecosystem, with 15% of PoW miners refusing the hard fork and the survival of this chain giving other constituencies (developer, users) a chance to also reject the fork. The chain which persisted with the consensus rules as they were defined became known as Ethereum Classic (ETC) - it lost the right to call itself Ethereum because that trademark was controlled by the Ethereum Foundation. The implications of this for the Ethereum commons have already been considered.

The hard fork was effectively a bailout, and the nature of the crypto commons is such that this kind of rollback is always possible if the stronger constituencies within a network are negatively affected. This can act as a kind of defence mechanism too, because an external attacker who wishes to destroy the network

cannot be assured that its constituents will not "fork around" them and their attack. This likely helps to discourage attacks which are very costly.

One of the lessons to be learned from the DAO is to be wary of complexity when dealing with blockchain-based assets. The "immutable" nature of these systems (when it holds) means that mistakes can result in catastrophic losses. If your autonomous organization is built on flawed foundations it can crumble in an instant. Greater complexity means it is harder to be sure that such flaws are not present, and there are great incentives for people to find them if they do exist.

In hindsight, it seems hard to believe that people were willing to entrust so much money to a brand new initiative that was deploying its very first iteration in the wild. Even without the fatal flaws, one wonders how well such an ambitious first attempt at a DAO would have made use of the resources which had been allocated to it. DAOs became less popular for a time after The DAO episode, but in mid-2019 we are witnessing a rapid proliferation of this form. This time around, even the DAOs that have been online for months or years are not being entrusted with more than a few million dollars, and we are yet to see compelling evidence that they will make efficient use of the resources that are allocated to them.

It has recently been announced that we will see an attempt to "resurrect" The DAO. A new attempt to build a DAO with the same objectives is forthcoming and will perhaps give us the opportunity to see how the concept fares when it doesn't get exploited at launch.

Moloch DAO

Moloch DAO is a smart contract DAO launched in early 2019 for funding development of the Ethereum ecosystem. Members in the DAO have non-transferable shares which they can use to vote on proposals. The DAO is funded by "tribute", when new members join they add resources to the fund. It is in a sense a DAO for collectively administering donations.

Proposals relate to minting new shares and assigning them to (new or existing) members in exchange for tribute (or promised work). Members vote to control who is allowed to join and how shares are issued. All members can cash in their shares for a proportion of the fund, but they then lose voting power. When a proposal passes, any members of the defeated minority who opposed it can withdraw their funds ("ragequit") before the proposal is paid out, leaving those who approved it to pay a larger proportion. This mechanism is intended to make the fund resistant to majority attack - if a majority approves a large payment for itself the minority can exit before they are diluted by this act. It may also serve to promote group cohesion, as members may avoid pushing or voting for a proposal if they believe it will cause other members to ragequit.

As of August 18th 2019, 85 Moloch DAO proposals have been completed, and

a further 10 are being voted on. Most of the proposals so far have been about granting membership (and some shares) to specific Ethereum community members. The standard issue of new shares is 100, for which people have been contributing an equivalent quantity of 100 ETH (~$20,000). Vitalik Buterin and Joseph Lubin both acquired 1,000 shares (and donated 1,000 ETH) each. Many proposals refer to applicants as numbered members of an organization (e.g. ConsenSys has 9 members, Ethereum Foundation has 10). In this initial phase the DAO is being seeded with members who are effectively hand-picked by the leaders in the ecosystem.

More recently, Moloch seems to be moving past the onboarding phase and there are a greater proportion of proposals to fund specific people/projects. The fund currently holds 7249 ETH (~$1.5 million) and has paid out ~$55k so far, most funded proposals are for <$10k.

Maker DAO

Below is based on (and quotes heavily from) an overview written by Seth Benton, as part of the crypto-governance-research project.

> The main goal of the MakerDAO is keeping the value of DAI, a collateral-backed cryptocurrency, stable relative to the US Dollar (i.e. a "soft peg" stablecoin). DAI is issued and managed through a system of smart contracts running on the Ethereum blockchain. MakerDAO governance is primarily concerned with the determining the risk parameters that are used to manage the portfolio of assets backing DAI (currently just ETH, but soon others with the introduction of multi-collateral DAI).
>
> MKR is Maker's "governance" token. MKR holders vote on proposed changes to the system via "voting contracts" (smart contracts running on the Ethereum blockchain). 1 MKR = 1 vote, and there are two types of votes: "executive votes" and "governance votes".
>
> Governance votes can be used to vote on one or multiple issues at once. They do not automatically trigger updates to the Maker system; these must be implemented via executive votes. Nor are they binding resolutions. Rather, they are used to poll community sentiment towards larger, more substantial changes to the system. This can include making changes to the structure or governance processes of the Maker Foundation, including adding new Oracles, adding a new risk team (people that create and apply risk models), or adopting a new voting process. Votes can be time-limited. If the vote is time-limited, votes are tallied at the end of the voting period and a simple majority (<50%) determines the outcome.
>
> Executive votes are a more common occurrence, and are used to

change the state, or "governance variables" of the smart contracts constituting the Maker infrastructure. Typically this means modifying the existing "risk parameters" of smart contracts that manage Collateral Debt Positions (CDPs), the debt instruments used to issue DAI and manage its supply. For example, an executive vote could be held to decide whether or not to raise the "stability fee" (i.e. "interest" paid to MKR holders on loans of DAI). Executive votes can also introduce new parameters or smart contracts. For example adding a new collateral type once multi-collateral DAI is launched.

Executive votes are binding. If passed, they are automatically implemented on the blockchain after a 24 hr delay (a measure to protect against hacks or governance attacks). Any Ethereum address can make a proposal and trigger a vote. However, in practice, since the MKR supply is currently centralized into the hands of a few key players such as the Maker Foundation and large investors, only executive votes created by the "core team" currently have a reasonable chance of passing.

For now, proposals for executive votes are created in a more traditional, centralized process within the Maker Foundation, utilizing the "Risk Governance Framework" detailed below, a formal process that attempts to emulate the scientific process. Feedback from MKR holders and the general "governance community" is taken into account at various stages. Maker's goal is to perform a "gradual decentralization" of this process over time as the system matures.

Maker has created an internal process that utilizes an objective "risk governance framework". In this process, "risk teams" (professionals employed by the Maker Foundation) utilize a formal, rigorous framework for continually evaluating the qualitative and quantitative risks associated with various collateral types. For instance the volatility risk, liquidity risk, and stability of the asset fundamentals. The outputs of this framework are then input into well-understood risk models borrowed from traditional finance to determine optimal "risk parameters" such as the debt ceiling, liquidation ratio, stability fee, and other parameters. The core team then presents their new models, data and suggested parameters to MKR holders and the community at large. Feedback from the community is incorporated and then put into a proposal for an executive vote. The executive vote itself can be used to gather further feedback from MKR holders, which can be incorporated back into the proposal. Eventually, MakerDAO intends to further decentralize this process, creating multiple risk teams elected by MKR holders that compete with each other using the risk governance framework, creating a "decentralized, open scientific risk management community".

In practice, this process seems to follow a fairly regular weekly ca-

dence. Risk team members answer questions about potential changes to risk parameters on a regular basis on Maker's chat and subreddit. Major decisions are typically debated and made during weekly MakerDAO Governance and Risk meetings, which are livestreamed and open to community participation via chat, then made available on YouTube and Soundcloud. Meetings and transcripts are made available on github. Typically, decisions made in Governance and Risk meetings are put to the community in Governance votes to poll sentiment, then put into Executive votes shortly thereafter unless governance votes reflect strong dissent.

Executive voting is not time-limited, but instead employs continuous approval voting. Whichever proposal currently has the most votes represents the current state of the system. There is no quorum, incentivizing MKR holders' continuous participation. At any time, a new proposal can be submitted to MKR holders (e.g. a proposal to lower the debt ceiling to decrease exposure to ETH). If it gains a majority of votes, it will be automatically implemented. The proposal contract is granted administrative access, and after implementing changes to the system, wipes its logic and cannot be reused. New proposals are not immediately implemented however. There is a 24 hr delay period, in which "Emergency Oracles" can trigger an emergency shutdown in the event of "long-term market irrationality", hacking, or security breaches. In multi-collateral DAI, Emergency Oracles will have the unilateral ability to trigger an emergency shutdown. This will give a minority of MKR holders the ability to trigger a shutdown if they believe the "governance community" (core team) is making off-chain decisions that have become biased or corrupted. For example, if large MKR holders try to get favorable risk parameters for an asset they hold to pump their bags.

Changes to existing risk parameters (variables in existing smart contracts) can be implemented automatically. Major upgrades involving changes to smart contract logic must be performed through the emergency shutdown process (i.e. rebooting the entire system).

The MKR token was launched on Dec 27, 2017. 1,000,000 MKR were premined. Maker did not ICO. In the early days, tokens were sold strategically by the Maker Foundation to members of the community, with preference given to early contributors to the project. Sales were largely negotiated on an individual basis in Maker's chat.

In 2017, the Maker foundation made its first institutional sale to Polychain Capital, a deal which was publicly negotiated with community input on the MakerDAO subreddit. Subsequent sales to other institutional investors such as Andreesen Horowitz, Placeholder VC, and others, were modeled on this deal, according to founder Rune Christensen in a podcast, where Maker distribution is discussed

generally.

While wider distribution of MKR is planned, MKR is fairly concentrated among a few key players. As reported in a CoinDesk article on March 6, 2019, according to Etherscan, the top three MKR accounts hold a combined 55 percent of tokens. At the time of the article's publication, the largest wallet, containing 27% of the supply, is a developer fund. This fund is controlled by a multi-signature wallet controlled by the Maker Foundation's board. According to MakerDAO community lead David Utrobin, the Maker Foundation's intention is to fully spend this fund "within the next few years". On March 15th (2019) David relayed in MakerDAO's chat that there were "around 270k MKR". In the article, several large MKR holders were asked for information on their holdings. Polychain capital confirmed it held "a significant portion" of MKR tokens. 6 percent is owned by Andreessen Horowitz's a16z fund. Hedge fund 1confirmation confirmed they are a "significant holder". The Ethereum Foundation and Ethereum co-founder Joseph Lubin declined to comment regarding their holdings.

Because MKR must be used to pay stability fees, and this MKR is burned upon payment, the supply of MKR is continually decreasing as CDPs are paid off. On Jan 29th, 2019, Rune Christensen estimated on a podcast that probably "less than 0.1% of the total supply" had been burned.

Rather than an initial coin offering, MKR tokens have already been minted and are being sold in an ad hoc manner by the Maker Foundation. MKR tokens are used to govern the Maker DAO, primarily to vote on setting the stability fee. Along with this rolling vote on the stability fee, MKR holders may also participate in polls. So far these are usually created by members of the Maker Foundation, which can be used to establish support for something that would be developed then put to a binding executive vote.

The Maker Foundation dominates Maker's governance, the MKR tokens are highly concentrated and several critical functions are the exclusive domain of people who work at the Foundation. By choosing to disburse MKR tokens on an ongoing basis the Foundation opted to slowly decentralize governance of the DAI stablecoin. Writing in August 2019, they seem to still be near the start of that journey.

The Maker DAO is like a central bank where votes are held to set the interest rate. Over time, the aim is to decentralize more of the functioning of the DAO. For now, voting rights are highly concentrated (3 wallets control 55% of tokens). This, coupled with the dominant position of the Foundation, means that Maker DAO is not being governed in a particularly decentralized way.

Maker has however become an important entity within the Ethereum ecosystem, with use of the DAI stablecoin deeply integrated into many Decentralized Finance

(DeFi) initiatives. The stakes are already quite high for Maker's governance, and it is likely that over time the Ethereum ecosystem will push for this to be further decentralized.

Blockchain for What?

> Permit me to issue and control the money of a nation, and I care not who makes its laws!
>
> Apocryphal Quote, 1838

A good blockchain is good at ensuring that network participants follow the rules, and that everyone who is interested can understand the rules and audit the chain. It minimizes the need to trust other parties, greatly expanding the ways in which parties who do not trust each other can interact productively. The big wins here are not having to trust the money issuer to implement their issuance policy as stated, and not having to trust intermediaries like banks to live up to their commitments. Adherence to the rules can be verified on the blockchain, access cannot be restricted because of the network's distributed peer-to-peer nature.

Because the blockchain's infrastructure is made from FOSS and a public record shared by thousands of nodes, it is impossible for a single authority to exercise complete control over any blockchain. Any subset of participants can create their own version of a blockchain at any time, modifying any rules or parameters they want to. This makes the form robust to dictatorial control without participants' consent.

Keeping the barrier to becoming a fully fledged participating node low means that there can be many of these. Easy access to full nodes is what makes these networks robust to any effort to shut them down.

Cohesion is an important consideration on the crypto commons, because there is little friction involved in forking a chain - it can happen accidentally. Any persistent chain split means a fragmentation of the ecosystem surrounding it. A blockchain is worth nothing if there are multiple conflicting versions of it and users cannot reliably differentiate which one to follow. Any split weakens network effects and diminishes the size and diversity of the ecosystem producing the common pool resource and giving it value.

It is better for everyone if consensus is maintained, and this makes herding a powerful dynamic. Entities have power on the crypto commons to the extent that they can steer their herd. Developers attempt to lead the herd, while miners corral it through the rules that they choose to enforce. The market signals "your assets will be worth $X if you do this, and $Y if you do that".

Through the lens of common pool resources: the cryptographic fabric of the blockchain allows for the rules to be enforced at any scale. Aside from a few

blips in the early years, Bitcoin has been reliably enforcing its consensus rules for a decade. After the tumultuous forking (and threats) of 2017, the social contract around what Bitcoin is seems to be more stable too.

Although robust enforcement of the rules is achievable, many blockchains have been successfully attacked, either through exploiting bugs in the software that enforces consensus (e.g. inflation attacks) or exploiting an opportunity to profitably deviate from the established social contract (e.g. double spend attack reorgs).

The crypto commons exist in a hostile environment, where significant actors would like to see these networks broken and abandoned. Projects compete with each other for recognition, participation, hashpower, adoption and market demand. Within the commons-based ecosystem for a project there may be significant infighting, where unresolved conflicts can simmer without a method of agreeing to change the consensus - until they potentially reach a point where some parties exit.

Many of these projects have a commons which is dominated by a single organization or small set of organizations, in which cases success depends on how well that organization performs. Longer term, in cases where decentralization is an important part of the value proposition, success also depends on whether the project can reduce its reliance on this central entity.

For projects that build tools for decision-making into their commons, the quality of those tools and how they are used is important and highly variable. Where important decisions are made by voting, the level of turnout for those votes matters. Where turnout is low, a small number of large holders can dictate the outcome of votes.

The distribution of voting rights is also important, the system can be only as decentralized as the voting power. Where a small number of actors could coordinate to exercise control over consensus or another aspect of decision-making, the blockchain loses its robustness to coercion and much of its value.

Human attention and the capacity to dedicate time to thought and participation is one of the most vital and constrained resources for blockchains that aim to decentralize their decision-making. This limitation, and the difficulties and costs associated with enabling large scale deliberation and decision-making (Nick Szabo's Social Scalability), are the basis of the doctrine that Bitcoin does not have governance.

Bitcoin does have governance, because it is a network run by people and those people have choices about which software they run and how that software implements the consensus rules. Developers have choices about which soft or hard forks they code up. The decisions of miners about which code to run are also very important.

Deferring to the judgment of a small group of well established contributors, along with a resolution that changes to consensus rules will be constrained to soft forks

which are unambiguous technical improvements - is a reasonable position to take in the absence of any way to empower the Bitcoin ecosystem to make collective decisions.

There is no mode of governance proven to work well for a decentralized blockchain in the long run (the long run just started), so the challenge is to invent one or hope that dogma can be used to paper over the cracks in rough consensus as practiced by other FOSS projects.

Resistance to change and minimization of the role of active decision-making is a valid strategy that could in many cases produce better results than adoption of more formal governance. The details matter, especially for on chain governance - who has voting rights, what are they trying to achieve, how are they coordinating.

My view is that developing commons-based decentralized governance for (and on) blockchains is vital to unlocking the technology's potential. The dominant cryptoasset networks will be those with the strongest production ecosystems. Weight of numbers counts but so does the capacity to effectively align the incentives of the parties who produce and manage the common pool resource.

Time spent arguing in a stalemate is time wasted. The disagreements between conflicting parties in a blockchain's ecosystem can be loud and vitriolic, as was the case with the block size debate, BCH hard fork and SegWit2x failure. When controversies arise, "no governance" looks more like a failure of governance, as various constituencies try whatever they can think of to tip the balance in their favor.

Formal governance has associated costs, and when a project is small this cost may outweigh the benefits. A formal approach to governance must be broadly perceived as legitimate by ecosystem participants or it will have limited use. It would be difficult to establish the legitimacy of formal governance which is added to a blockchain that is already up and running, because this will inevitably diminish the power of some constituency and that constituency is likely to reject such a change. My view is that the strongest governance can be achieved with an approach that is present from the genesis of a blockchain, at least in the form of a principle embedded in the social contract. There are many examples of blockchain communities who lack an established method of decision-making and are now struggling to make collective decisions (see Ethereum and Zcash for some recent examples).

When the principles of governance are established *a priori*, all network participants implicitly accept these principles when they decide to engage. This provides a strong foundation for governance, for as long as the method of governance presented at the outset is adhered to. Projects like Decred and Tezos have incorporated methods of changing their rules which extend to changing the decision-making process itself. In principle, this offers a level of flexibility which should allow for the legitimacy of this method of decision-making to be maintained.

Delegation is an important aspect of decision-making on the crypto commons - it is impractical for every stakeholder to reason and vote about every decision. With DPoS this delegation is a formal delegation of decision-making power or sovereignty, establishing a class of governors who make decisions on behalf of a broader stakeholder group that elects them. As all block reward incentives flow to or through the elected delegates, and rewards equate to more votes, they will have opportunities to entrench their position.

With pure PoW systems the miners have responsibility for implementing the rules of the network faithfully, but they may have little social authority to instantiate rule changes. This can lead to conflict with other stakeholders who watch and ensure that all blocks comply with the rules that have been collectively agreed for the network.

Delegation also happens to the degree that users (uncritically) follow the roadmap or plan of a particular dev team. An ecosystem with one set of active developers and limited critical oversight of their work has effectively delegated all decision-making to those developers. Critical oversight from a large set of knowledgeable stakeholders is a strength, but open dialogue at scale in a public space is noisy and easily infiltrated by provocateurs. Methods to reduce or cut through the noise are important, but this is a difficult problem to solve and there are trade-offs with any approach.

One advantage of formal decision-making is as a means of organizing the community's discourse and moving past contentious issues. Without an agreed upon method of making important decisions, it can be difficult for participants to know what the true degree of support for a plan is within the ecosystem - whether it genuinely lacks support or is being strategically blocked by some of the less transparent entities.

Even within decentralized decision-making systems with broad participation in voting, voters may vote primarily based on their trust in what another community member has concluded, or based on consideration of the points others have raised, rather than their own research and reflection. There is however an important distinction between this kind of soft deference to respected others and explicit delegation of sovereignty that empowers another to act on one's behalf. It makes the difference between leaders enjoying influence and leaders enjoying (largely unfettered) power.

The most important resource for these projects internally is the attention of their stakeholders. When decision-making power is decentralized there is a larger pool of participants who must spend time to understand and engage with the decisions being made. Delegation in various forms is one way to address this, there are also some interesting examples with concepts like Futarchy where prediction markets are used to incentivize a constituency of predictors to figure out what the stakeholders would or should vote for, then delegate some degree of power to that prediction market driven entity.

The essential aim of decentralizing decision making power is to address the weak-

ness of centralized points of failure, but in practice the decentralized decision making entity must also make good decisions. Each project competes with others across a range of aspects, and performance on generalized indicators such as adoption and price matters to virtually all of them. Projects that decentralize decision-making need methods of doing so that maximize the collective intelligence of the participants. To succeed, they must make and execute better decisions than both their decentralized competitors and projects with more centralized leadership.

To the extent that the decision-making of a project is decentralized, the attitudes and beliefs of its constituents will shape the course it takes. In addition to the number of participants and the amount they invest, the strength of their alignment around shared goals is also important. As are the details of the shared goals themselves.

What would you call a large scale decentralized network of peers that provides an important public resource globally, and demonstrates collective intelligence and cohesion in doing so? I feel like we're going to need a better taxonomy for these things, because once a model is established and demonstrates that it works, there's no putting that genie back in the bottle. My guess is that there are going to be a few of these entities that really shake things up, hopefully for the better, but "better" means different things to different people.

This is a time when new blockchain-production-related organizational forms are proliferating and natural selection is beginning to exert its influence. The objective function of this selection is based on what people like you and I demand, what you but also your voice in the decision making milieu of whatever projects you take an interest in. Voice means different things in different projects, sometimes it means shouting (and liking) into the social media void (along with bots and sockpuppets, as well as other people), sometimes it means electing a representative to participate on your behalf, and sometimes it means direct participation in a decision making process or picking up a keyboard and getting involved in producing something.

This kind of activity in aggregate will determine what the potential of blockchain technology amounts to. We are just learning about it but it seems to be quite versatile, and it is there on the commons to be shaped into useful forms. If it happens on the commons, participation is permissionless. All of this stuff is open source, a small team can make something novel with the available building blocks.

Commons based peer production is driven by the doers, people who want something badly enough to contribute to building it. Blockchains allow us to build global ledgers that cannot be corrupted or shut down and which people cannot be prevented from accessing (provided a minimal degree of hardware, connectivity and freedom).

Commons Based Economy

If "software is eating the world", then the means of producing that software will come to define the new epoch. Proprietary software and walled gardens controlled by corporate entities represent the transfer and emulation of industrial era practices into the "digital economy". Top-down control within the corporation means that the constraints of profitability are imposed above all other considerations. As the role that some of these big tech companies fill has become more like the provision of important public utilities, it has become clear that they are generally not very good at performing this role. The frequency of damaging hacks and misuse of data is testament to this.

Commons based peer production is native to the internet, it represents the way in which people can efficiently work together on a larger goal when communication costs are reduced to effectively zero. It is an excellent choice for the production of non-rival goods, where use by one party does not restrict use by others. With present levels of communications technology the category of non-rival goods has expanded to include all software, digital media and information resources.

Blockchains are a new kind of commons, bringing together permissionless access with digital scarcity to create money and other assets that are globally accessible and easily transferrable. The blockchain commons is made with FOSS, and *can only be* made with FOSS. It puts open source software development projects at the centre of important global networks providing valuable services.

Some blockchains can fund their own development, they are self-sustaining digital organisms, incentivizing participation by all of the constituencies of contributors that they need to survive and thrive. Blockchains that have resources to fund their own development tend to conceive of this quite broadly, going beyond the writing of code to incorporate a variety of other activities which work towards the project's aims.

The aims of these projects go beyond producing good software, often involving grand ambitions to fundamentally change how people conduct aspects of their lives, or modify aspects of the socioeconomic system. This means that the funding these projects dispense goes towards a range of activities which will strengthen their commons in a variety of ways.

This is a novel funding mechanism for commons-based peer production, which outside the domain of FOSS has been even more hampered by the difficulties of funding the production of public goods.

DAOs are an effort to build methods of coordination into the commons. Organizations that can be trusted to implement the rules of decision-making in the way that has been agreed by all participants. This idea has the potential to transform our capacity to organize by minimizing the transaction costs associated with doing so, improving efficiency and diminishing risks when collaborating with people who are relatively unknown (and therefore untrusted).

Effective DAOs are already here. For example, the Decred stakeholders collectively control a Treasury fund with around 660,000 DCR ($15 million), and also have strong methods for enforcing and amending the network's consensus rules. It is funding the production of this resource, along with a variety of FOSS projects (including blockchain daemons, wallets, block explorers), and the production of a variety of other media (you're reading some of it right now). Where they are well designed, these decentralized entities will be resilient and long-lasting. It is likely more useful to think in terms of how great or small the successes will be with different approaches than about absolute success or failure. The only outright failure occurs when virtually all participants choose to abandon the network, which usually comes after a slide into irrelevance. The success stories will be unstoppable, and could be highly significant.

Software is Hard

Our software infrastructure for handling data and security in general is poor, as evidenced by the many breaches of personal information and ransomware attacks. The adapted industrial method of organizing software development has a lot of issues. The health and profitability of the producing organization comes first, the software is a means to that end.

There is an expanse of room to improve upon the organization of software production and the means of incentivizing this. In my view it is important to look after the intrinsic motivation of workers, especially software engineers and especially those who are working on public infrastructure. When people are working on vital infrastructure which is only understood by a relatively small number of contributors, it benefits us all if they are dedicated to the cause of maintaining it well.

Cryptocurrency emphasizes security and robustness, relying on an incentive scheme and ironclad method of enforcing the rules to attract participants who will build and maintain the network and cultivate its resource.

FOSS blockchain projects are examples of hard software, which exists in an adversarial environment where there are great rewards available to anyone who can exploit a flaw. All of the code is open, relying on the principle that "with enough eyes all bugs are shallow". The prospective rewards are incentives for people to look for those flaws, with bug bounty programs and audits offering ways for white hat hackers to also participate and be rewarded for strengthening security.

Cryptocurrency is FOSS-native, and many of these projects are adept at generating funding to support their own development through various means. This addresses one set of limiting factors for FOSS projects generally, in particular where key personnel can receive funding to work directly on the code without being distracted by other tasks.

As funding is a key constraint for FOSS projects generally, control of development funding for cryptoasset projects means significant influence in their governance. For this reason, a number of projects are attempting to solve the problem of how to decentralize control of development funding, and make the developers accountable to some other constituency.

There is significant promise in the idea of DAOs for funding and coordinating software production, and there are enough high-stakes experiments in motion now that we'll find out how well this really works over the next few years.

If there is a generally applicable method to incentivize and reward high quality contributions to digital infrastructure, we all stand to benefit greatly from identifying and adopting it.

If it works for FOSS, there's no reason it wouldn't also work for other forms of CBPP. Anything that could work well as a commons-based public good (which as far as I'm concerned is all digitizable media) could find utility in new modes of production that leverage DAOs.

We will see how this works first in the cryptocurrency domain, because cryptocurrencies are socio-digital organisms that print money to incentivize their own upkeep and expansion. Centralization is a weakness for these organisms, and so the selection process should favour those projects which minimize or isolate that weakness, in the long run.

There is competition to advance the decentralization of governance on the crypto commons, as these advances are made some aspects will be applicable to the governance of other types of public goods and common pool resources.

At the Crypto Crossroads

Software is infinitely reproducible, but good software remains a scarce commodity. When software for a specific task is required, options are limited and there is no guarantee of their quality. Access to this software may come at a cost, denominated in money or one's personal data.

Cryptocurrencies have shown anyone who's paying attention that the digital commons offers new affordances for producing digital money or assets. My thesis is that the means of production of these common pool resources is as significant as the resources themselves, when considering the trajectory of blockchain technology or the cryptocurrency movement over the long term.

In my view we are at something of a crossroads in the crypto space, where major players in the "legacy" economy are starting to take an interest in blockchains. They may throw significant resources into their own blockchain-based efforts, to try and claim mind and market share from the more commons-native upstarts. They may attempt to capture established projects by buying key organizations or infrastructure providers.

Libra is an effort instigated by Facebook to apply the principles of blockchain to decentralize control of a currency among 100 corporations, each paying $10 million and being approved by the Libra Association. Telegram (messaging app) are running an ICO which has already taken in $1.7 billion in private investment before opening for a limited public sale. The bet which investors in these projects are making is that tech companies which have already captured significant numbers of users on social platforms will be able to leverage this to funnel their users into adopting their cryptocurrency or blockchain offerings.

The combination of significant VC funding and ICOs with big roles for the VC-backed entity also serves as a way to transplant the established players and ways of doing things (and their capital) onto the crypto commons.

In my view the VC-style approach is ill-suited to the crypto commons. Projects that grow organically and build out their commons-based infrastructure as they do so have a natural advantage because it is easier for them to become (more) decentralized.

However, these projects feed on attention, and it is possible that good projects will be starved while poor projects persist because they have assets which can be used to capture mindshare and market cap. If people predominantly follow and buy assets with shaky foundations which subsequently deteriorate or reveal themselves as centralized - this would be a setback for the whole concept.

The potential for the blockchain-enabled commons is huge, and there are any number of possibilities for how this new technology could be used. We are witnessing a Cambrian explosion in experiments with this technology and digitally native organizational forms to go with those experiments. Most of these experiments will likely fizzle out, they all have global ambitions and cannot simultaneously realize these. By 2025, most of 2019's experiments will likely be forgotten, some concepts will be written off entirely, and there will no doubt be new experiments pushing new boundaries that we cannot yet foresee.

Blockchain projects that are still expanding their commons productively in 2030 will I expect be highly significant, perhaps as much as the tech giants are today or on the road to that kind of importance to human society.

To the extent that these projects are truly commons-based, everyone is permitted to observe how their experiments play out and learn from their observations. The nature of the commons limits the power of gatekeepers to control who can participate in these projects, although in practice FOSS governance can entrench respected figures in positions of power.

Self-funding blockchains have the potential to bring the idea of a "FOSS movement" into play on new terms, where the issues with funding and incentivizing development are effectively solved. The ideology this time is not so much about the software as the sovereign networks it brings into being, each of which has its own specific aims. A community or ecosystem of participants coalesce around those aims and work together to try and achieve them, they stand to benefit

individually and as a group from success.

The digital commons and CBPP are a prerequisite for any of this to be possible, and projects which embrace and make good use of the commons will derive strength from this. I believe that success will be determined by the scale of the ecosystem interacting with how well participating constituencies are aligned and their capacity to coordinate efficiently towards achieving shared goals.

Blockchains are like digital organisms, composed of code, a social contract about what the network is for and how it works, and a way of incentivizing people to run, maintain and develop the network. They thrive on attention and interest, and for as long as at least some people want to run a decentralized network, it will be available in some capacity.

As of mid-2019 speculation is a major driving force, as individuals seek to buy assets which will appreciate the most in value going forward, and price or market capitalization are key metrics to gauge success.

The undercurrents which will determine the technology's long term direction are less visible, they are formed by the choices of the doers and builders about which projects they will contribute to, by the level of coordination between the set of contributors to a project and by how well that project's aims align with the technology's strengths.

We should be considering which networks we feed with attention, who is providing that attention and input, how those people are interacting with the networks, and what they aim to achieve. The answers to these questions right now are shaping perceptions of what the blockchain and cryptocurrency movement is about - they will determine which of the potential blockchain futures come to pass.

Cryptocurrency affords us the opportunity to move part of our digitally recorded life off the servers of the big finance and tech corporations, outside of their oversight and discretion. Cryptocurrencies with fixed issuance offer an opt out from the inflationary monetary policies of states.

Blockchain technology can offer this commons-based alternative in other domains. We are already seeing movements like #DeFi (Decentralized Finance) and experiments with social networks that aim to provide commons-based alternatives to relying on large centralized corporations.

What we learn about decentralization of control and governance on the crypto commons will echo in other domains where these are desirable characteristics.

Conclusion

This is the end, thanks for reading! There are three things I would suggest as key takeaways:

- The blockchain space is worth watching if you're interested in social production or digitally native means of production.
- Commons based peer production and common pool resources are useful lenses through which to observe the space - the paradigm is that blockchains are a revolution in how we use the digital commons and are shaking up the incentives for participating in commons-based peer production.
- Look at how decisions are being made within these projects. If governance is decentralized and permissionless you should be able to find where it is happening and participate in that process.

If you read this all the way through I would appreciate any feedback you have to offer.

Cheers,

Richard Red

Powered by the Academic theme for Hugo.

Cite ×

Copy Download