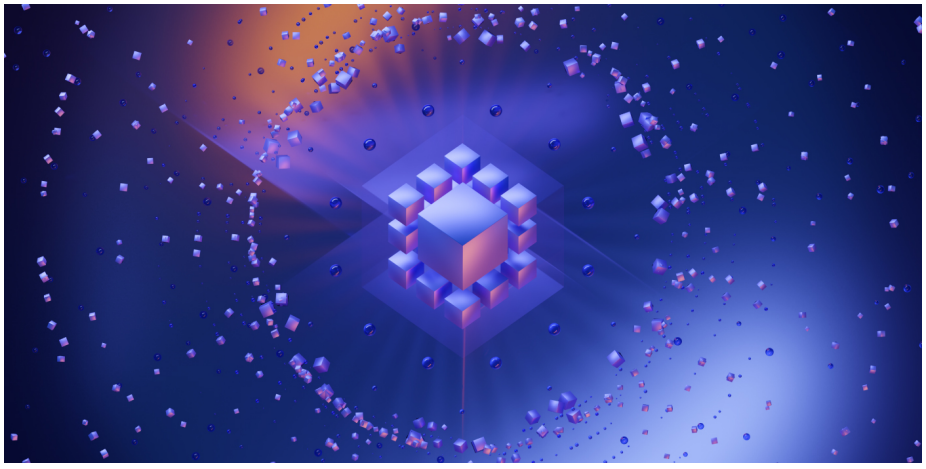
Peer Production on the Crypto Commons

Search

Introduction



Introduction

This book/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 blockchain ecosystems will be explored.

Free and Open Source Software (FOSS) is behind most of the digital public infrastructure we rely on when we use the internet, and offers compelling alternatives to proprietary software in almost every domain. Commons-based peer production includes FOSS and also other types of information resource that are freely available and produced by their community - including Wikipedia, OpenStreetMap and the Pirate Bay.

The book presents 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.

Cryptography strengthens the digital commons by allowing people to build things that are robust to attack. It has opened up a new range of possibilities for the kind of commons-based resources that can be produced, and the ways in which these resources can sustain themselves.

Bitcoin is a resilient social organism, native to the crypto 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 kind of 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. These dynamics will determine how the network behaves in the long run as it encounters obstacles and seeks to overcome these.

Blockchains are actively constructed by their human participants, who can be considered as a set of constituencies that each do their part to add value to the network and its native assets (i.e. Bitcoins). Once the assets a blockchain tracks have been established as holding value, the network pays for its own upkeep by awarding newly minted coins to the workers who maintain it (i.e. Proof of Work miners), as well as allowing these workers to collect transaction fees from users. A higher price for the asset means increased purchasing power for the network as it mints coins and allocates these to the workers who provide security.

There are two key constituencies driving every blockchain network: the developers of the blockchain's software infrastructure, and the producers of blocks on the network (miners). The book considers how these constituencies interact

with each other and the other constituencies that contribute to producing and adding value to the blockchain's commons. These other constituencies include merchants, service providers, funders, node operators, users, and storytellers.

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 providing the capacity to make uncensorable transactions) is finite. Scale comes at a cost to nodes in the network, more transactions means more data to process and more records to store.

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. They incentivize the production effort in new ways and they allow participants to create robust digital entities together. 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.

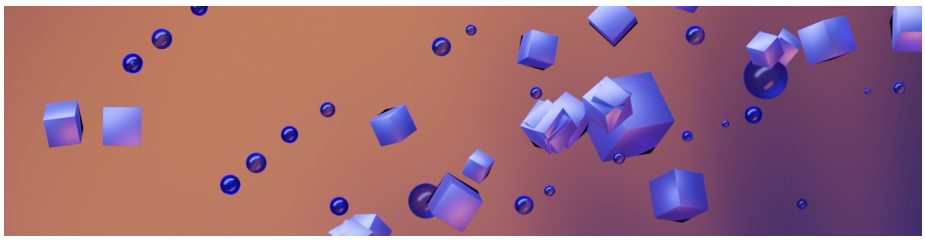
The first part of this resource introduces the concepts and considers what is familiar and what is different about the cryptocurrency context. A framework is developed which involves profiling the constituencies that make up a blockchain's ecosystem and considering the roles they play and how they interact 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. The aim of the second part is to record observations about what is happening on or to the various crypto commons. These observations demonstrate how to apply the framework and the kind of insights that can be gained by viewing blockchain communities in terms of constituencies working on a common pool resource.

Decentralized Autonomous Organizations (DAOs) have emerged as an effort to harness the coordination and organizational affordances of blockchains. Towards the end the book considers 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 1.0 - released Jan 3 2021, the first version to be publicly released was v0.8 on Nov 1 2019.

Commons Based Peer Production (CBPP)



Yochai Benkler wrote about the concept of commons-based peer production in his 2006 book "The Wealth of Networks - How Social Production Transforms Markets and Freedom"[1], 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 access to 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 [2] 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 [3], relies on open allocation internally. Spotify also uses[4] 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 [1]. 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 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 revenues and profit from its sale or deployment - these revenues 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.

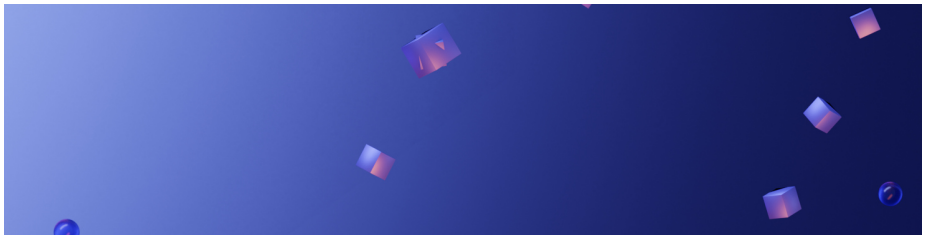
There is much more to a cryptocurrency than the FOSS which participants in

the network run, but many of the other forms of work which go into producing a cryptocurrency and giving it value can also be considered as forms of CBPP.

References

1. Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press. Online at: https://cyber.harvard.edu/wealth_of_networks/Download_PDFs_of_the_book
2. Eghbal, N. (2016). *Roads and bridges: The unseen labor behind our digital infrastructure*. Ford Foundation. Online at: https://www.fordfoundation.org/about/library/reports-and-studies/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/
3. Microsoft has acquired GitHub for $7.5B in stock. (n.d.). *TechCrunch*. Retrieved 8 November 2020, from https://social.techcrunch.com/2018/06/04/microsoft-has-acquired-github-for-7-5b-in-microsoft-stock/
4. *Spotify Engineering Culture (by Henrik Kniberg)*. (2017, February 27). https://www.youtube.com/watch?v=4GK1NDTWbkY

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[1]. 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) 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, or those servers being taken offline).

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) have been growing quickly, often following a strategy of subsidizing the service until it can gain a dominant position in its market, before beginning to extract the value from those users and their data.

The point of this simplistic overview is to establish that **the question of how software development and digital infrastructure is funded has become an important one for human society**. Software is penetrating many walks of life, and the question of how its development and maintenance 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* [2]. In this article, Coaese considered why organizations form and hire employees when the production they engage in could be contracted out. An efficient market would allow for the organization to exist as a nexus of contracts, but in practice the transaction costs are prohibitive.

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.

References

---

1. Raymond, E. (1999). The cathedral and the bazaar. *Knowledge, Technology & Policy*, *12*(3), 23–49. https://doi.org/10.1007/s12130-999-1026-0 Free version at: http://www.unterstein.net/su/docs/CathBaz.pdf
2. Coase, R. H. (1937). The Nature of the Firm. *Economica*, *4*(16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

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[1]) 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) [2] 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)[2]

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[3]

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)[4] 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[3] 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.

References

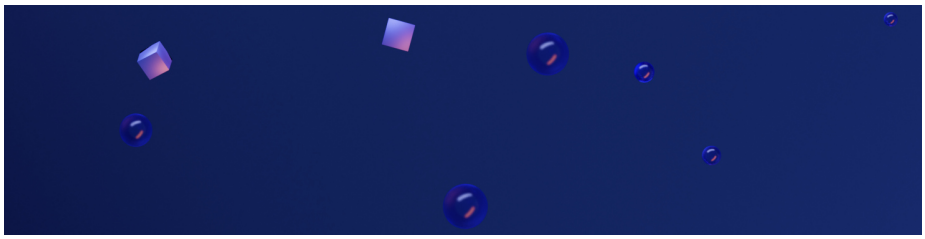
1. Deci, E. L. (1972). The effects of contingent and noncontingent rewards and controls on intrinsic motivation. *Organizational Behavior and Human Performance*, *8*(2), 217–229. https://doi.org/10.1016/0030-5073(72)90047-5

2. Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, *125*(6), 627–668. https://doi.org/10.1037/0033-2909.125.6.627

3. Roberts, J. A., Hann, I.-H., & Slaughter, S. A. (2006). Understanding the Motivations, Participation, and Performance of Open Source Software Developers: A Longitudinal Study of the Apache Projects. *Management Science*, *52*(7), 984–999. https://doi.org/10.1287/mnsc.1060.0554

4. Lakhani, K. R., & Wolf, R. G. (2003). *Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects* (SSRN Scholarly Paper ID 443040). Social Science Research Network. https://doi.org/10.2139/ssrn.443040

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 diminishes the role of 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. This necessitates a 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[1] in terms of a digital panopticon that would allow 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 one 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. This complexity limits 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"[2] 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[2] 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[3], 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.

In 2020 Microsoft Office 365 deployed a new Productivity Score feature[4] which tracks workers actions such as emails sent, files read, meetings attended (with and without camera) and sends reports about their productivity to managers. At a time when people were working from home much more, the surveillance capacity of the product could be swiftly expanded. There has been significant pushback[5] against the feature.

Motivated Workers

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, or adapting to the organization's culture, as well as just working hard.

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.

Technical Debt and Bullshit Jobs

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 hard 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[6] 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[7]) considers what constitutes a bullshit (pointless) job, how many people think they have one (~37-40%[8]), 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. Box-ticking appraisals diminish intrinsic motivation and divorces success at work from the quality of one's work product.

References

1. Scheiber, N. (2019, July 3). Inside an Amazon Warehouse, Robots' Ways Rub Off on Humans (Published 2019). *The New York Times*. https://www.nytimes.com/2019/07/03/business/economy/amazon-warehouse-labor-robots.html

2. Cohan, P. (2012.). *Why Stack Ranking Worked Better at GE Than Microsoft*. Forbes. https://www.forbes.com/sites/petercohan/2012/07/13/why-stack-ranking-worked-better-at-ge-than-microsoft/

3. Mims, C. (2013). *Google engineers insist 20% time is not dead—It's just turned into 120% time*. Quartz. https://qz.com/116196/google-engineers-insist-20-time-is-not-dead-its-just-turned-into-120-time/

4. Sandler, R. (2020). *Microsoft's New 'Productivity Score' Lets Your Boss Monitor How Often You Use Email And Attend Video Meetings*. Forbes. https://www.forbes.com/sites/rachelsandler/2020/11/25/microsofts-new-productivity-score-lets-your-boss-monitor-how-often-you-use-email-and-attend-video-meetings/

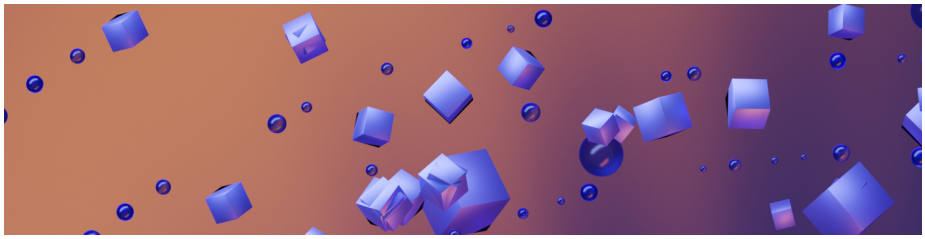
5. O'Flaherty, K. (2020). *Microsoft's New Productivity Score And Workplace Tracking: Here's The Problem*. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2020/11/29/microsofts-new-productivity-score-what-does-it-mean-for-you/

6. Chris Dannen, Leo Zhang. (2018). *What's Really Driving the Cryptocurrency Phenomenon?* Iterative Capital Management. http://iterative.capital/thesis/

7. Graeber, D. (2019, February 7). *Bullshit jobs: The rise of pointless work, and what we can do about it* [Monograph]. Penguin. http://eprints.lse.ac.uk/100858/

8. Bullshit jobs and the yoke of managerial feudalism. (2018, June 29). *The Economist*. https://www.economist.com/open-future/2018/06/29/bullshit-jobs-and-the-yoke-of-managerial-feudalism

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. If the people in charge of a particular version of the software make decisions that colleagues or users disagree with (e.g. new UI), those who reject that direction can opt out. There is no copyright restriction to prevent 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.

Many participants in FOSS projects work on them part-time and do not need to generate an income from this work. FOSS projects that are not integral to the operations of organizations with resources to fund development have limited scope to generate money to pay contributors. In these cases most contributors will tend to 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[1] 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 with this business model reaching a large size ($3.4 billion revenue in 2018).

FOSS software development may also be funded by grants from funding bodies or through government spending. The European Commission is decidedly pro-FOSS, having since 2000 a strategy for promoting internal use of FOSS and stipulating that software funded by its research and innovation actions should be FOSS wherever possible.

Nadia Eghbal has written an excellent and comprehensive report on the unseen

labor behind our digital infrastructure [2] which explores the prevalence of open source code in our digital infrastructure. The report paints a picture of freely provided commons-based digital infrastructure that is often not being looked after by its main beneficiaries.

Eghbal's report describes several in depth examples of widely used important FOSS which is maintained on a shoestring budget by people who are stretched. The Heartbleed OpenSSL bug is one well known example, the library used by a majority of https sites had a significant undetected exploit for a number of years. 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.

One of the issues Eghbal identifies is that the people who drive FOSS projects forward typically do not want to spend time trying to secure or administer funding for the effort. The success stories usually involve other people who step in to source and administer funding that allows the engineers to be compensated for their work with minimal distraction. The question of **what kind of support structures help FOSS projects flourish** is an important one, and is considered from a number of angles in the rest of the resource.

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, without necessarily embracing the more ideological component of software that is "Free Libre".

The disconnect between FOSS utility and funding has been receiving more attention[3] lately. 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 a rare example of an organization that gains a lot from FOSS deciding to give something back to support the commons.

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.

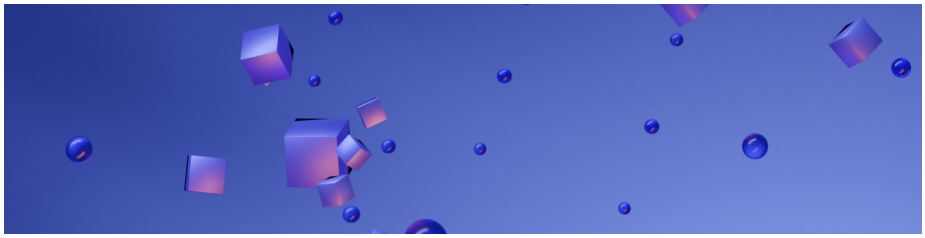
References

1. Red Hat Becomes Open Source's First $1 Billion Baby. (n.d.). *Wired*. Retrieved 22 December 2020, from https://www.wired.com/2012/03/red-hat/

2. Eghbal, N. (2016). *Roads and bridges: The unseen labor behind our digital infrastructure*. Ford Foundation. https://www.fordfoundation.org/about/library/reports-and-studies/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure

3. Oberhaus, Daniel. (2019). *The Internet Was Built on the Free Labor of Open Source Developers. Is That Sustainable?* https://www.vice.com/en/article/43zak3/the-internet-was-built-on-the-free-labor-of-open-source-developers-is-that-sustainable

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[1] only one explained how its governance worked in any detail, with 62% saying nothing at all about this. In 2018 [2]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, conflict is easier to manage. 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 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[3] 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 its strengths. Mako Hill calls for better tools to facilitate ongoing relationships between forks.

For most FOSS projects, governance is minimized because most of the volunteer participants in the project do not want to spend their time engaging in lengthy discussions. For maintainers of a project making group decisions about its future is part of the more general task of coordinating contributions, which can become burdensome for projects with many contributors.

References

1. Cabot, J. (2016, January 15). *Transparency and Democracy in open source: Not what you thought.* Livable Software. https://livablesoftware.com/transparency-democracy-open-source-not-thought/

2. Canovas, J. (2018) *Projects that make their rules explicit would see more participation.* Opensource.Com. https://opensource.com/open-organization/18/4/new-governance-model-research

3. Hill, B. M. (2005). *To Fork or Not To Fork: Lessons From Ubuntu and Debian: Benjamin Mako Hill.* https://mako.cc/writing/to_fork_or_not_to_fork.html

FLOSS On the Ropes

In 2020 Nadia Eghbal's new book, *Working in Public: The Making and Maintenance of Open Source Software*[1], was released. I was happy to see the scope expand from *Roads and Bridges* to incorporate Commons Based Peer Production and the governance of common pool resources, the work of Benkler and Ostrom featuring heavily. It also benefits greatly from Nadia's time at GitHub, with reams of interesting stats about how the platform is being used by open source communities. I heartily recommend this book for anyone with an interest in how contemporary open source infrastructure is created and maintained.

One of the trends Nadia's work highlights is the decline in prominence of the FLOSS (Free Libre Open Source Software) ethos, which is quite anti-corporate, in favour of a more apolitical adoption of Open Source as a generic best practice. The dominant role corporations have come to play in some domains of OSS are making it clearer who the primary beneficiaries are, economically at least, and this is giving some contributors cause to pause and consider where it's all headed. Mozilla has been a major player in open source, offering the most viable alternative web browser to the more surveillance-friendly android backed by Google and co., but had to lay off[2] 250 workers this year due to "coronavirus-era revenue declines".

The general sense seems to be that the Free Software movement has been dead for a while, with the GNU GPLv3 licensing debate[3] and outcome turning out to be a pivotal moment in its decline. In 2007, some advocates of Free Software wanted to prevent the "Tivoization" of FOSS, where hardware manufacturers could use it within products that restricted the freedom of users to further modify that hardware and software after buying it through forms of imposed lock-in. The GPLv3 license in 2015 accounted for just 8.88% of GitHub repositories[4], lower than GPLv2 (13%), with GPL now less commonly used than the more permissive MIT license (45%).

It seems that there is growing disillusionment now with the state of the Open Source commons, it has been colonised by corporate interests and many contributors are feeling like their work is exposed to be picked up by companies whose adoption will generate a lot of work and responsibility for the project but probably little revenue.

Intrinsic motivation usually covers the creation of code because coders like to make new things, but maintenance is another story. Now we have come to

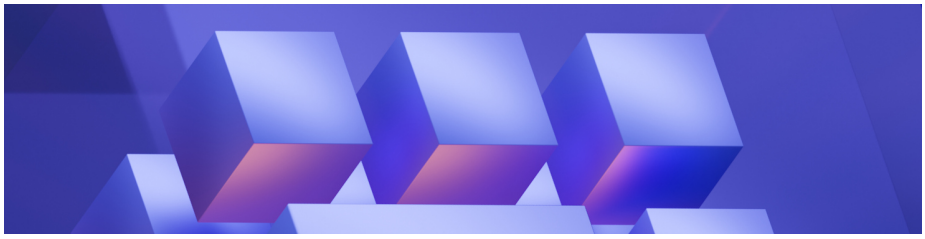
depend on open source software for much of our communications, but there has been a lack of consideration paid to the web of dependencies underpinning many popular web applications and the people who keep all of those packages and libraries working and secure.

The following sections look at FOSS in the crypto space, where the context and scene is very different.

---

1. Eghbal, N. (2020). *Working in Public: The Making and Maintenance of Open Source Software*. Stripe Press.
2. Melendez, S. (2020). *Mozilla vows MDN 'isn't going anywhere' as layoffs cause panic among developers*. Fast Company. https://www.fastcompany.com/90539632/mozilla-vows-mdn-isnt-going-anywhere-as-layoffs-cause-panic-among-developers
3. Babcock, C. (2007). *The Controversy Over GPL 3*. InformationWeek. https://www.informationweek.com/the-controversy-over-gpl-3/198001444
4. Balter, B. (2015, March 10). Open source license usage on GitHub.com. *The GitHub Blog*. https://github.blog/2015-03-09-open-source-license-usage-on-github-com/

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. Malicious or exploitable cryptocurrency wallet software puts all of the user's assets stored in the wallet at risk.

Open Source software is preferred in 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 a 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.

Consensus Rules

Cryptocurrencies 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 in the same network. This is achieved with a set of rules which allow all the nodes 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. The stability and security of the distributed

ledger is important to the blockchain's value proposition. The consensus rules are the nodes' way of agreeing on which of any conflicting chains is the definitive and legitimate one. In Bitcoin's case, the rules state that the legitimate Bitcoin chain is the one with the most accumulated Proof-of-Work that follows all of the other rules.

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. 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 from 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 option 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. Where a hard fork is uncontroversial the whole network migrates to a new rule-set at the same time and the chain with the old rules fails to progress because all of the block producers have moved to the "new" network.

If the hard fork is controversial some users may choose to reject the change and persist with the old rules. If a chain following the old rules is to survive, it is critical that there are enough miners or block producers among its supporters to continue making new blocks at a reasonable pace.

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 about how to scale up. The BCH faction 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. Nodes following the old rules do not reject blocks with SegWit transactions because they don't break Bitcoin's consensus rules. However, nodes that do not update will not be able to properly interpret SegWit transactions because they rely on additional rules being enforced. Soft forks only require miners to adopt the new software for the amended consensus rules to take effect for all network participants.

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[1] (following a more basic introduction to concepts like PoW). Here's another article introducing the differences from Coindesk[2].

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 for Bitcoin 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.

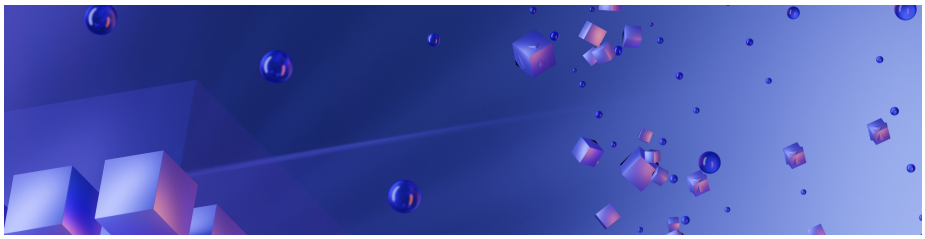
"No hard forks" has implications for technical debt, as it restricts the options available to developers who wish to upgrade the network. In effect, Bitcoin developers must maintain backward compatibility with software from 2010 (see here[3] for a list of Bitcoin consensus forks).

References

---

1. Red, R. (2018, April 11). *Ch. 4 Soft forks, hard forks, chain splits and free coins!* in*A User Perspective and Introduction to Blockchain Governance*. Block Commons. https://www.blockcommons.red/post/user-perspective/
2. Castor, A. (2017, March 27). *A Short Guide to Bitcoin Forks*. CoinDesk. https://www.coindesk.com/short-guide-bitcoin-forks-explained
3. BitMex Research (December 2017). *A complete history of Bitcoin's consensus forks | BitMEX Blog*. https://blog.bitmex.com/bitcoins-consensus-forks/

Bitcoin Cash Hard Fork



Bitcoin scaling debate

The Bitcoin scaling debate which ultimately led to Bitcoin Cash was a long and drawn out affair. This detailed account[1] by Daniel Morgan describes a fundamental disagreement between two factions of Bitcoin developers. One of these factions wanted to pursue the ideal of "peer to peer electronic cash" by increasing the block size limit so that more people could use Bitcoin without fees increasing. The other faction opposed block size increases as a way to scale, and saw the development of a fee market for block space as essential to Bitcoin's long term survival.

It is interesting to note that the Bitcoin whitepaper was a key text in this discourse, with the idea of "Satoshi's Vision" acting as a banner to rally supporters of the big block ideals that ultimately found their embodiment in Bitcoin Cash.

Satoshi Nakamoto would have been a strong contender for Bitcoin "benevolent dictator for life" if they had stuck around - at least for as long as the identity was operated by people with coherent views, if it was in fact a group effort. This is probably one of the reasons they disappeared, recognizing that having such a figure may not be in Bitcoin's best interests.

Without the persona to arbitrate, readings of the white paper and Satoshi's other writings became ammunition in the conflict. The whitepaper is a key document in Bitcoin's social contract, because it pre-dates the network and serves as a specification of what the network is for and how it should be operated. Everyone who has ever used Bitcoin has implicitly agreed to this social contract as initially described in the white paper and implemented then iterated in the Bitcoin node software.

As the scaling debate progressed, all parties agreed that Bitcoin in its current state could not scale to become an everyday payment option, because the number of transactions it could process would not be sufficient for such regular use by many people.

Big blocks were intended to maintain low fees per transaction by allowing for more of them. However, significantly bigger blocks would lead to the hardware requirements for running a Bitcoin node to increase significantly. This would result in fewer nodes, weakening the network's decentralization and security.

The alternative scaling approach was to focus on Layer 2 solutions, off-chain mechanisms for transacting in Bitcoin without leaving a heavy on chain footprint. The most well known Layer 2 scaling solution is Lightning Network, where on chain transactions are used to open channels and create a balance which is spendable within the lightning network. Implicit in this approach is the idea that on chain Bitcoin transactions are more weighty things that should be used only when significant amounts are involved.

Miners generally appeared to be supportive of block size increases. By keeping this activity on chain the transaction fees would all accrue to the miners and a

higher cost of nodes would be insignificant compared to their mining hardware and operational costs.

To complicate matters further, the soft fork SegWit change which was needed to allow Lightning Network to be used safely would also break "AsicBoost". AsicBoost was an exploit which Bitmain, the main manufacturer of ASICs, were thought to be leveraging to gain a competitive advantage[2].

Miners first blocked the activation of SegWit, maintaining the status quo for quite a long period of time. Eventually, Bitcoin developers and users mobilised to force the miners to adopt SegWit or see the chain split and a significant faction of the ecosystem reject their blocks for failing to offer this support (see UASF episode in developers section).

Bitcoin Cash: A Competitor is Born

Bitcoin Cash (BCH) was born at Bitcoin block height 478,559 (on 1 August 2017), when the faction of the Bitcoin ecosystem which rejected SegWit and preferred to scale the block size introduced its own hard fork change to the consensus rules and split the Bitcoin chain. 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[3] algorithm as part of the hard fork, a drop in hashpower was predicted (because most mining power signalled support for BTC). BCH 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[4].
- 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 one expects to be worth more in the future, is the one to buy, and determines which software to run and which chain to follow.

In November 2018 the BCH chain was deliberately split again[5], to form BCH ABC (now recognized as the winning BCH by most exchanges) and BCH Satoshi's Vision. The Bitcoin Satoshi's Vision chain was established largely on the principle of following "Satoshi's Vision" for Bitcoin, as the name implied. Craig Wright was a leading figure, and he claimed to be Satoshi, and therefore an authoritative figure on the subject of what Satoshi's vision for Bitcoin is.

More recently, the BCH ABC chain split again accidentally[6] 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.

In 2020, the BCH (ABC) chain was split again on philosophical/economic grounds[7], with the developers of the ABC node software adding a "development tax" of 8% of the block reward, which is diverted from the PoW miners' 100% share. This was quite an unpopular proposal among vocal BCH community members, and 80% of miners had signalled support for an alternative version without this tax. Once the time came for the fork, the minority of hashpower BCH ABC had quickly disappeared completely and the chain died. Bitcoin Cash will have no block reward funding of developers.

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, the availability of alternatives, and the project's social contract.

References

1. *The Great Bitcoin Scaling Debate—A Timeline | Hacker Noon.* (2017). https://hackernoon.com/the-great-bitcoin-scaling-debate-a-timeline-6108081dbada

2. Rizzo, P. (2017, April 6). *Bitcoin's New Controversy: The AsicBoost Allegations Explained*. CoinDesk. https://www.coindesk.com/bitcoins-new-controversy-asicboost-allegations-explained

3. Aggarwal, V., & Tan, Y. (2019). *A Structural Analysis of Bitcoin Cash's Emergency Difficulty Adjustment Algorithm* (SSRN Scholarly Paper ID 3383739). Social Science Research Network. https://doi.org/10.2139/ssrn.3383739

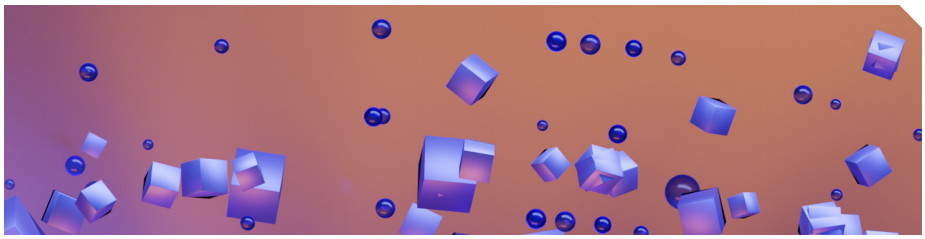
4. Buntix, J. P. (2017). BCH EDA Was Designed to Cause Bitcoin Network Congestion, Former Dev Claims. *The Merkle News*. https://themerkle.com/bch-eda-was-designed-to-cause-bitcoin-network-congestion-former-dev-claims/

5. Red, R. (2018, November 26). *Hash War Theater*. Medium. https://richardred.medium.com/hash-war-theater-67d3fcac3e97

6. Bitmex Research. (2019). *The Bitcoin Cash Hardfork – Three Interrelated Incidents | BitMEX Blog*. https://blog.bitmex.com/the-bitcoin-cash-hardfork-three-interrelated-incidents/

7. Frost, L. (2020, November 16). *Bitcoin Cash Hard Fork: Here's What Happened*. Decrypt. https://decrypt.co/48409/bitcoin-cash-hard-fork-heres-what-happened

FOSS for Common Pool Resources



With the coordinated participation of a number of constituencies, blockchain FOSS can become the backbone of a powerful network that can transmit information and value globally 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)[1] 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 mean more honest hashpower competing for those rewards, making it more difficult to amass enough dishonest hashpower to successfully attack the network.

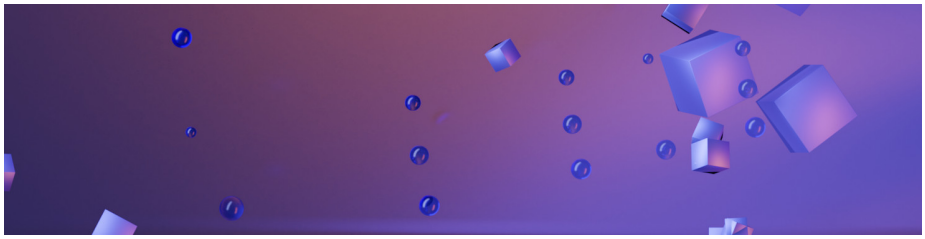
This section will consider distributed ledgers as common pool resources, applying the framework of Elinor Ostrom as presented in Governing the commons: The evolution of institutions for collective action[2]. Ostrom's work is concerned with avoiding the tragedy of the commons, and she looks at how groups of people aim to do this in a variety of contexts, looking beyond conventional state and market approaches at successful management of real resources.

References

---

1. Hasu. (2019, January 15). *Unpacking Bitcoin's Social Contract*. Medium. https://medium.com/s/story/bitcoins-social-contract-1f8b05ee24a9
2. Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

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[1] - 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. Ostrom looks specifically at self-governance of common pool resources by their users, distinct from state or market-based approaches. 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[2], 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. Cryptography is key to this capacity, because it makes it much easier for defenders of the network to verify the authenticity of information than it is for attackers to introduce corrupt information.

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 available block space is a good example of this. It effectively creates an open fee market for block space, which is a robust low-complexity solution. Determining the block size limit is a key decision for the people producing the Bitcoin resource, it's akin to a community deciding how big a fence they want to build around their commons grazing land - bigger might be more profitable, but it's harder to maintain. The mining constituency were keen on the whole keen to expand the area during the "scaling debate", but the developers as a constituency, who are responsible for long term maintenance, were less keen to expand as this would make it harder for regular users to run a node and "tend to the commons".

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 cryptocurrency.

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.

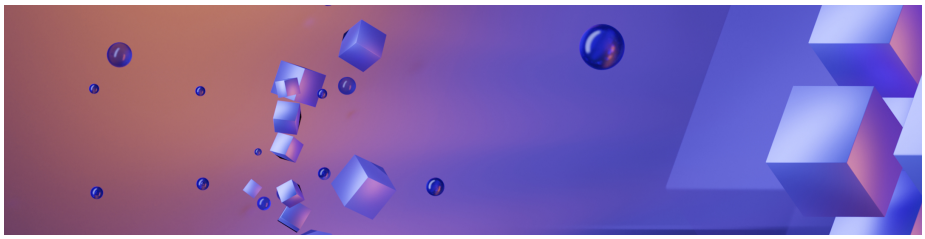
Bitcoin's consensus rules cover the use of the common pool resource well, otherwise it would not have survived and thrived for 10 years. They do not however address how the common pool resource should be further developed. This creates problems, because everyone agrees that the resource does need further development of some sort or other.

References

1. Hardin, G. (1968). The Tragedy of the Commons. *Journal of Natural Resources Policy Research*, *1*(3), 243–253. https://doi.org/10.1080/19390450903037302

2. Song, J. (2017, August 12). *Understanding Segwit Block Size*. Medium. https://jimmysong.medium.com/understanding-segwit-block-size-fd901b87c9d4

Crypto Club Goods?



In 2020 some interesting tweets from Hasu and others prompted me to look more closely at what kind of resource the blockchain is, and pointed me to an article by Conrad Graf [1] which makes an interesting case for "Club Goods" as the type of economic good which is the closest match to the type of economic good that is bitcoin/cryptocurrency.

This argument rests on the idea that block space is a non-rivalrous good, one person's use of the good does not affect whether someone else can also use it. In this framing the restriction of block space creates artificial scarcity, the Bitcoin network operators have introduced a way to make what was a natural public good excludable - by controlling who can access it and charging a fee to do so (transaction fees).

	Excludable	Non-excludable
Rivalrous	**Private goods** food, clothing, cars, parking spaces	**Common-pool resources** fish stocks, timber, coal
Non-rivalrous	**Club goods** cinemas, private parks, satellite television	**Public goods** free-to-air television, air, national defense

Figure 1: Types of Economic Goods, from Wikipedia

I don't agree that space on the Bitcoin ledger is non-rivalrous, because without limitation (no block size limit and therefore very low or no transaction fees) a tragedy of the commons would quickly unfold, with rapid bloat in block size and increasing traffic resulting in a reduced number of publicly accessible nodes.

Instead, my view is that the Bitcoin developers realized the rivalrous nature of block space early on when they introduced the block size limit, well before it

was really needed, to ensure that this vital resource at the heart of the Bitcoin commons could not be over-used and depleted carelessly (people making too many transactions and resulting increase in difficulty to sync a node).

In practice none of these types are an exact match though. I would say it's not right to characterise Bitcoin as excludable because by design the network cannot police who is using it, node operators cannot exclude anyone in particular. It's also not entirely non-excludable, because there is a requirement to hold BTC and pay fees to transact using the Bitcoin ledger.

In my view this is the Bitcoin developer constituency building our the infrastructure in a way that prevents over-use of the resource, like a tap on an irrigation system that can only flow at a maximum rate - while the miners seem more keen to increase the flow rate (block size).

From a consumer perspective however, there is a price on admission to block space and people who spend more can get more transactions in - which is more like a club good. Anyone can be a member of Club Bitcoin, as long as they've got enough BTC to pay miners to include their transactions.

Holding BTC and using it to make Bitcoin transactions makes one a Bitcoin user, which is distinct from playing an active role in the creation and maintenance of the (common pool) resource. Running a Bitcoin node is a minimal form of participation which is useful because it helps with relaying transactions quickly, and because node operators can help to validate the work of PoW miners. However, node operators who cannot deploy hashpower and mine blocks don't have any power to do anything else to intervene in cases where something is suspicious except raise the alarm.

The main actors on the Bitcoin commons are the miners who compose blocks and the developers who write the software everyone uses. Miners have significant influence on chain but they have little influence over the other vital constituencies like developers and economic nodes. "Economic nodes", such as those operated by major exchanges or service providers, can have major influence too, in particular around chain splits.

"Club goods" fit well with private ownership because the owner exercises control over who has access and this enables them to collect rents. It is Bitcoin's lack of control over the boundaries of the resource which makes it permissionless to access, and the same issues apply to social aspects like governance. As the New York Agreement episode showed, you can have a private meeting about Bitcoin's governance, but the fact that it was private was held against it by many Bitcoin community members who fought against implementing Segwit2x as the agreement described.

What it comes down to for me is that running and maintaining the Bitcoin network and ledger, looks more like managing a common pool resource than a club good.

If artificial scarcity makes Bitcoin a club good, does it mean that a cryptocurrency like Nano, which doesn't have a block space limit, and which doesn't have fees for transactions, is a public good?

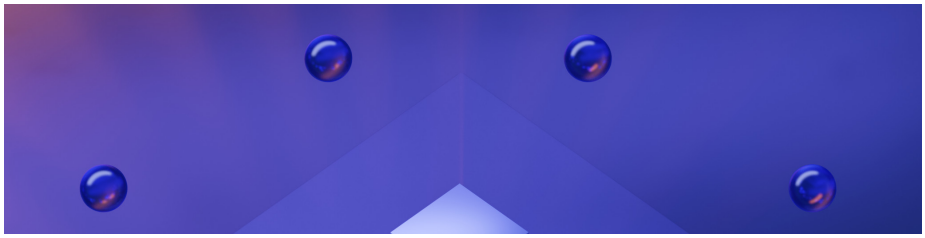
I would say no, because there's still a requirement to have a NANO balance to transact with, which is a barrier to public use. The economics are different however, without a block size limit or transaction fees it becomes easier to use Nano with a very small balance, but the down side is that the validators are effectively providing Nano users with a free service. This is vulnerable to a tragedy of the commons, where validators may have to find a way to make their work profitable or stop doing it.

References

---

1. Graf, K. S. (2019). *The Bitcoin Block Size Limit, Artificial Scarcity, and Code-Enhanced Public Club Governance*. 18. https://www.konradsgraf.com/blog1/2019/12/24/new-paper-the-bitcoin-block-size-limit-artificial-scarcity-and-code-enhanced-public-club-governance

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)
- Users who run full nodes provide oversight to ensure that other participants follow the rules
- Users also create demand for the asset, and having more users increases its utility. When enough users choose to hold on to rather than spend the asset, they reduce the amount which is availabile to buy, generally leading to price appreciation.

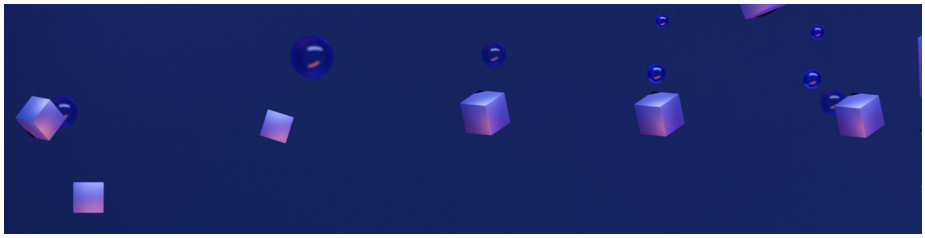
The value of the cryptoasset is important for every network where it is used to incentivize block producers, because it determines the network's security budget.

A network's security budget is in basic terms defined by the size of the rewards 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 and the direction in which it develops.

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 (by 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. A paper[1] by Hasu, James Prestwich and Brandon Curtis considers the question in some detail, in light of a new model of Bitcoin's security.

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[2] 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 un-spendable 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[3] 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[4] 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.

Miner Extractable Value and Dark Forests

In 2020 DeFi has provided many examples of Ethereum's PoW miners using their position to gain advantage over other users. The strategies available to miners for exploiting Decentralized Exchanges running on Ethereum have been documented and observed in the wild already in 2019[5].

There are two posts which give a developers' perspective of dealing with this "dark forest" environment (referencing the "Three Body Problem" science fiction series) as they tried to "rescue" some vulnerable funds after discovering an exploit which allowed anyone to claim them. The issue here is that miners could pick up any transactions that claim "free money" and instead of relaying that transaction swap in their own address as the beneficiary.

In the first one[6], by Dan Robinson and Georgios Konstantopoulos, the protagonists try to sneak a burn transaction past the mempool bots which they suspect are lurking, but it got picked off in a few seconds and the miner pocketed $12,000. The second[7] story on this subject, from samczsun, had higher stakes, benefitted from lessons learned in the earlier attempt, called in expert help, and was ultimately successful in the rescue of $9.6 million which had been sitting in a vulnerable smart contract by enlisting the help of a miner who could mine the transaction directly. I thought both of these were well written and interesting accounts of the true nature of the Ethereum mempool and one of the ways in which miners exert control over the network.

How secure is Proof of Work?

This article[8] 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. However, there are other factors which affect the miners disposition and level of skin in the game, such as whether their hardware is new or soon to be obsolete.

GPU miners are less exposed to a single asset 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.

References

1. Hasu, Prestwich, J. & Curtis, B. (2019) *A model for Bitcoin's security and the declining block subsidy* https://uncommoncore.co/wp-content/uploads/2019/10/A-model-for-Bitcoins-security-and-the-declining-block-subsidy-v1.05.pdf

2. Bitmex Research. (2019). *The Bitcoin Cash Hardfork – Three Interrelated Incidents | BitMEX Blog.* https://blog.bitmex.com/the-bitcoin-cash-hardfork-three-interrelated-incidents/

3. *Bitcoin Cash Miners Undo Attacker's Transactions With '51% Attack'.* (2019, May 24). CoinDesk. https://www.coindesk.com/bitcoin-cash-miners-undo-attackers-transactions-with-51-attack

4. Bitcoin History Part 10: The 184 Billion BTC Bug | Featured Bitcoin News. (2019, March 1). *Bitcoin News.* https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/

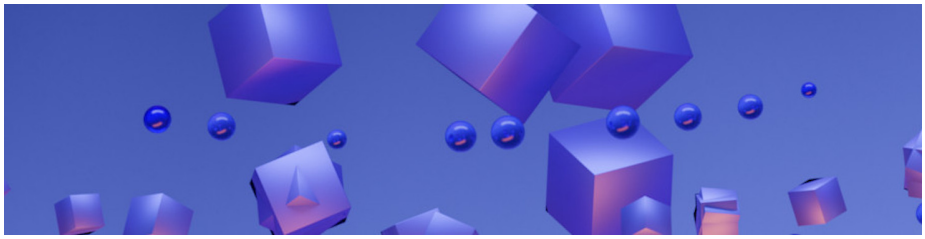
5. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv:1904.05234 [Cs].* http://arxiv.org/abs/1904.05234

6. Robinson, D. & Konstantopoulos, G. (2020, September 21). *Ethereum Is a Dark Forest.* Medium. https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff

7. Samczsun. *Escaping the Dark Forest.* (2020, September 24). https://samczsun.com/escaping-the-dark-forest/

8. Vorick, D. (2018, May 14). *The State of Cryptocurrency Mining.* Medium. https://blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b

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' capacity to reliably produce robust software 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.

User Activated Soft Fork

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

vated Soft Fork (UASF)[1]. The Bitcoin Core developers coded a set of updates and 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.

Miners are Influenced by Markets

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 drawn out 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.

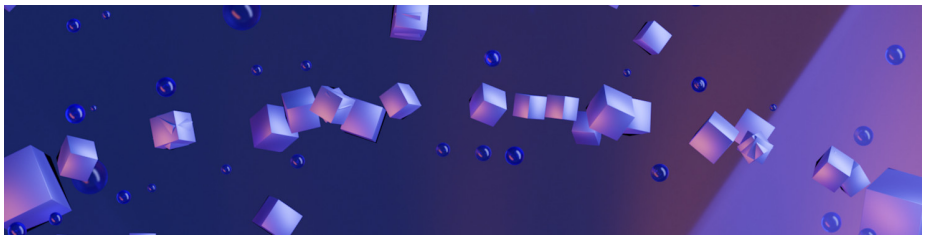
When the developers have the users/merchants/businesses on their side, 2017 indicated that they can rely on the market to control the power of miners. Market dynamics around cryptocurrencies are famously volatile however, and in the case of a more contentious split than Bitcoin Cash one might anticipate even more erratic behavior in the markets. This kind of event is not conducive to the use of cryptocurrency as currency, where stability and predictability are desirable characteristics. It is therefore not in the interests of any of the ecosystem participants for the governance process to behave this way and have these effects.

References

---

1. Song, J. (2017, August 12). *Bitcoin, UASF and Skin in the Game.* Medium. https://jimmysong.medium.com/bitcoin-uasf-and-skin-in-the-game-7695031c5689

Blockchain Development Funding



Miners are well rewarded for the role they play in securing the network. Merchants have built a business which relies on the network to function. 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).

The motivations of the engineers who write the software the network runs on are not as clear. 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).

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.

Since I wrote this section originally the subject of Bitcoin and blockchain development funding has been visited by a number of other researchers:

2019-10-31: An analysis of developer funding in Bitcoin published by Derek Hsue, Su Zhu, Hasu, & Brandon Curtis. This essay makes some of the same points as the following sections, with more detail and focus on Bitcoin's history. [1]

2020-03-28: BitMEX Research compiled a list of 17 organizations funding Bitcoin research and development, defined broadly to include projects like Lightning Network. Entities funding the most developers are Blockstream, Lightning Labs, Square Crypto (mix of in-house LN devs and sponsoring Bitcoin Core devs), MIT Digital Currency Initiative and Chaincode fund 6-8 developers each. [2]

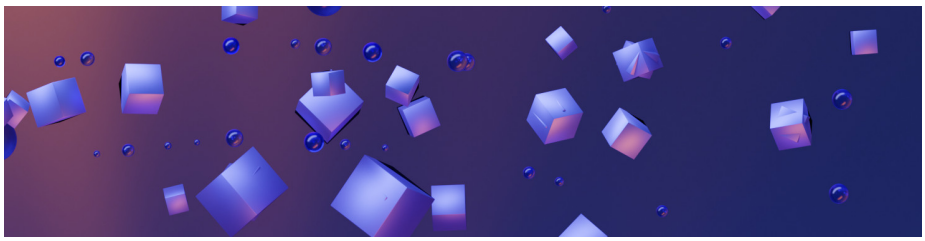
References

---

1. Hasu, & Hsue, D. (2019, October 31). *An analysis of developer funding in Bitcoin*. Deribit Insights. https://insights.deribit.com/market-research/an-analysis-of-developer-funding-in-bitcoin/

2. BitMEX Research (2020). *Who Funds Bitcoin Development? | BitMEX Blog*. Retrieved 24 December 2020, from https://blog.bitmex.com/who-funds-bitcoin-development/

Developer Holders



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 push the development of a blockchain project in the direction that they see fit. Dependence on an external party for income may mean deferring to that party's judgement about the direction development takes.

Historical Context

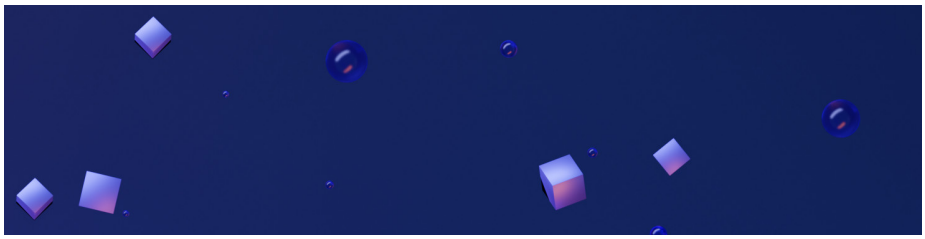
Early cryptocurrencies could be mined effectively with a variety of consumer hardware, in the early days CPUs were sufficient, later GPUs came to dominate mining and later ASICS (specialized chips which only mine a particular set of cryptocurrencies) were developed. As better hardware becomes available, 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.

In 2020, new evidence emerged that "Patoshi", the dominant PoW miner in Bitcoin's early stages who is thought to be Satoshi and have mined and held about 1 million BTC, also utilized multi-threading, whereby a miner can more efficiently use their hardware by searching for multiple nonces simultaneously. This innovation was not included in the publicly released code, suggesting even Satoshi was not above holding back some inside knowledge to gain an advantage.

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.

Associated Services



As with other forms of FOSS, one way to fund development work is through provision of services associated with the software.

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. It also employs a large number of prominent Bitcoin Core developers.
>
> The company has raised $76M to date from investors, including venture capital firms Horizons Ventures and Mosaic Ventures. - 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.

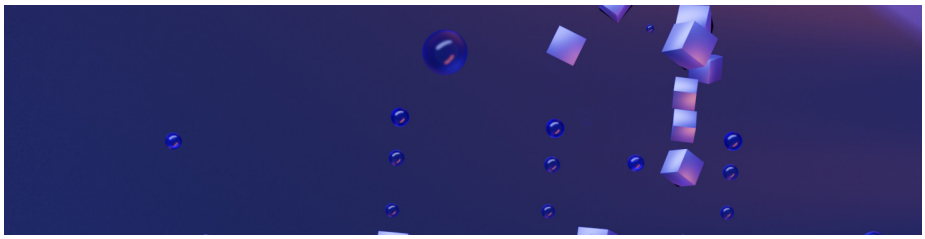
It is worth noting that Blockstream's efforts to enhance Bitcoin go beyond the Core software and its own revenue-generating products to encompass things like an array of satellites continually broadcasting the entire Bitcoin blockchain. These allow a user anywhere in the world to obtain the data and 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 (Aug 2019), Blockstream revealed that it had been growing its own PoW mining operation since the issue with PoW miners over SegWit in 2017 (see here). This is quite an interesting development, as it entails a major entity in the developer constituency also becoming a significant player in the mining constituency.

It is this spill-over 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".

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[1]. 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 (as adjudicated by the core team), 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.

Patronage, whereby developers are supported financially by benefactors, has taken on an increasingly important role in the funding of Bitcoin development work in recent years [2].

In 2012 the Bitcoin Foundation was formed to support Bitcoin development and uptake, it funded a number of Core developers in a patronage type arrangement until it ran out of funding in 2015.

MIT's Digital Currency Initiative stepped in to support Bitcoin development [3] at this point and continue to support some Bitcoin developers. Funding from academic or non-profit institutions is a familiar source of FOSS funding, and there are other non-profits funding aspects of Bitcoin development, like Chaincode Labs. A variety of ecosystem actors also support development of particular aspects when it matches their business objectives.

Corporations that are visible supporters of and dependant on Bitcoin have started to fund the people who work on it more. A 2020 article by BitMEX Research [4] lists a variety of initiatives which fund one or more Bitcoin developers.

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) [5] 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.

In Sep 2019 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 could vote for the project they would like to donate to, and each vote awarded 0.02 BTC (worth around $200). After one week the campaign's donation total stood at 0.56 BTC, with a total of 28 votes being cast far. When the campaign closed only 47 votes had been cast (worth 0.94 BTC), but OKCoin boosted the amount donated to 20 BTC.

Jack Dorsey has announced[6] 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.

More recently some of the largest cryptocurrency exchanges (Coinbase [7] and Kraken) have launched similar initiatives which fund developers working on various aspects of crypto commons infrastructure.

This article [2] by Nic Carter hails Bitcoin's Patronage system as an unheralded strength, and celebrates the significant improvement which has occurred in the last few years, during which time funding has expanded beyond Blockstream and MIT to encompass a wider range of patrons and also to projects beyond Bitcoin Core. The message that Bitcoin development needs funding for Bitcoin to succeed is reaching the entities who benefit from Bitcoin and seek to build it into their businesses - it is their responsibility, and more of them are now stepping up. The article also criticises projects with dedicated funding for development from the blockchain, and in many cases those criticisms are valid.

When it comes to decentralization, blockchains which have a dominant corporate entity are inferior to those without such an entity calling the shots. Patronage by the companies which rely on Bitcoin is better than a single ICO or block reward funded company dominating development, but I think it's setting one's sights too low to suggest that it's the best possible way to fund development of the crypto commons. I'm less sceptical of the role for this kind of patronage now than I was 2 years ago, now that it's happening at a more reasonable scale, but I think we need to see how it goes over the next few years as all of the recently announced or implemented funding streams develop and interact.

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.

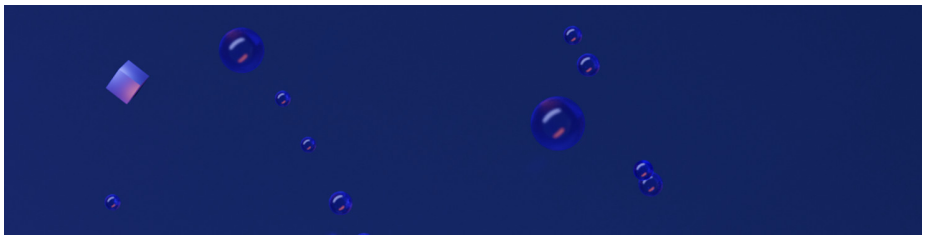
Donations are by their nature not a very reliable source of income, because they typically depend on the ongoing generosity of beneficiaries who are external to the production effort. There are also other more generic avenues open to open source developers, such as Patreon and GitHub's own service for linking maintainers with patrons. Gitcoin is somewhere between the fiat and crypto crowd-funding initiatives, adding "quadratic funding" and some centralized gate-

keeping around that to the donations/patronage model. Gitcoin is considered in a later section.

References

1. Wong, J. I. (2017). *Andreas Antonopoulos got $1.5 million in bitcoin donations after Roger Ver 'bitshamed' him—Quartz*. https://qz.com/1151233/andreas-antonopoulos-got-1-5-million-in-bitcoin-donations-after-roger-ver-bitshamed-him/
2. Carter, N. (2020, August 6). *Nic Carter: Bitcoin's Patronage System Is an Unheralded Strength*. CoinDesk. https://www.coindesk.com/bitcoins-patronage-system-is-an-unheralded-strength
3. Hasu, & Hsue, D. (2019, October 31). *An analysis of developer funding in Bitcoin*. Deribit Insights. https://insights.deribit.com/market-research/an-analysis-of-developer-funding-in-bitcoin/
4. BitMEX Research (2020). *Who Funds Bitcoin Development? | BitMEX Blog*. https://blog.bitmex.com/who-funds-bitcoin-development/
5. *'Hard Core Fund' Collects 50 BTC to Support Bitcoin Developers*. (2019, June 19). CoinDesk. https://www.coindesk.com/hard-core-fund-collects-50-btc-in-china-to-support-bitcoin-developers
6. *Square Is Hiring New Crypto Engineers—And It Wants to Pay Them in Bitcoin*. (2019, March 20). CoinDesk. https://www.coindesk.com/square-hiring-crypto-engineers-bitcoin
7. *Coinbase Awards Its First Round of Bitcoin Developer Grants*. (2020, December 23). CoinDesk. https://www.coindesk.com/coinbase-awards-first-round-bitcoin-developer-grants

Storytellers



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. After 10 years of doing its thing with only minor interruptions, Bitcoin is establishing itself as a firm presence in the global economy. People are using it as intended, probably quite a few people. In Oct 2019 the IRS was estimating that 12 million Americans owed tax on cryptocurrency transactions or had assets they needed to declare.

What are people using Bitcoin for? That is hard to say, because people buy, hold and exchange Bitcoin for a variety of reasons and there is a lack of good data on what their motivations are.

Telling us what Bitcoin is for is therefore the domain of storytellers, who are also responsible for distilling a highly technical construct (blockchain) down into a relatable form. There are a lot of different ways to look at Bitcoin, and different people will find the hook that gets them to take a closer look in different facets.

For a minority of transactions (those associated with criminality) Bitcoin's resistance to seizure and censorship would be the critical features. Bitcoin was for some time portrayed as the "currency of the dark web", primarily used for illicit purposes. This is still quite an influential narrative, that it serves black/grey market purposes and is used for money laundering. Cash and digital fiat currency are also used for these purposes, cryptocurrency may have some advantages in this regard but the use of a public distributed ledger to record all transactions in perpetuity must surely count as a significant down-side.

That narrative became less saleable when "respectable" institutions started to show an interest in Bitcoin. Here are some other plausible stories for why people buy and use Bitcoin:

- To use in transactions that are otherwise more expensive (e.g. cross-border payments).
- To use in transactions that one doesn't wish to be recorded by one's bank.
- As an alternative to holding a bank account.
- To circumvent capital controls.
- Lack of trust in local authorities to protect wealth stored in other ways.
- To hold for its fixed supply and ultimately deflationary economic properties, in the belief that it will be a good store of value.
- To hold in speculation that it will be worth more and can be sold at a higher price, as part of a short term trading strategy.
- To hold as an escape route or opt out of a local currency which has significant inflationary issues.
- For ideological reasons, believing a move to decentralized currencies to be in society's best interests.

The stories about why people use it define what it is for, and therefore narrative becomes an important component of governance on the crypto commons. If Bitcoin's rules are to change, that change has to make sense to its constituents, to fit in with their visions of Bitcoin[1].

The priority afforded to different use cases (electronic cash, store of value, global

reserve currency, tool for the oppressed) determines one's view on how development should proceed, what the priorities are and which trade-offs are worth making.

Narrative can also used as a weapon against cryptocurrencies by external actors who do not wish them to succeed. Nic Carter has a lot of great commentary[2] about the mainstream media's coverage of Bitcoin. It seems to have focused largely on price and the criminality angle, and it is rare to see any coverage that gives an indication of why so many people are interested in the idea.

Another popular narrative is that cryptocurrencies aren't backed by anything. Cryptocurrencies are backed by the belief that they will be around in the future, still available to all and working as intended, reliably following the rules of their social contract. The social contract for fixed supply cryptocurrencies states that the supply will decrease over time and eventually there will be no more issuance of new currency. People who expect this scarcity, coupled with increasing demand, to lead to price increasing over time, hold cryptocurrency as somewhere between a speculative asset and a "Store of Value".

The storytellers disseminate their versions of the narrative and social contract the way they see it. They buy into the story and understand that achieving their vision of cryptocurrency's place in the world depends on spreading the word to people who are unaware or ambivalent. Within the ecosystem, the same stories serve to bolster the cohesion of stakeholders around a shared version of the narrative and steer its governance accordingly.

This article[3] published in Oct 2019 considers Bitcoin as a new breed of "Headless Brand", with users having collective responsibility and individual freedom to define the brand. It provides an insightful overview of the decentralization of the branding component a cryptoasset, and considers the implications of commons-based brand production.

Narrative Control

The storytellers that people listen to are important, so too are the places where they tell their stories. Although the discourse is generally public, much of it happens on platforms where access to participate is (or can be) restricted. The /r/bitcoin subreddit for example is widely regarded as having quite heavy-handed moderation, where voicing support for certain perspectives on Bitcoin or cryptocurrency is likely to result in a ban.

On Twitter, where much of the Bitcoin and cryptocurrency debate seems to happen, some well known Bitcoiners routinely block other users for voicing opinions which go against their version of the Bitcoin story. The "social layer" is important for Bitcoin, because ultimately Bitcoin needs its users to be united around a shared understanding of how it should work. When well known and respected people voice opinions which are contrary to the dominant Bitcoin narrative, they are in effect weakening the consensus at the social layer.

Some Bitcoiners have adopted the position that this kind of deviation should be rejected or punished, and offenders should be excluded/blocked or harassed and harangued. The subject of memetic warfare has been presented at "true" Bitcoin conferences - How to Meme Bitcoin to the Moon.

When governance is informal it is difficult to draw a boundary around it, it permeates every facet of the ecosystem. When different factions form supporting different choices, this redraws the contours and boundaries of the commons and can turn them into a conflict zone.

Living on the Crypto Commons

There are now a significant number of people who spend most of their working or free time engaged in some aspect of the blockchain space. There are many people out there who care deeply about some blockchain or cryptocurrency project, to the point where it has become a significant part of their identity.

Nic Carter has described Bitcoiners as peaceful revolutionaries[4], and there are no doubt many who see themselves as such. Some people just want the number to go up so they become more wealthy, some (also) want to see a particular vision of global Bitcoin adoption come to pass, or have ambitions for how it will reshape some aspect of the economy or broader society. The prevailing attitude is one of looking at some broken aspect of society (like money), and asking whether it's possible to build an alternative that's better, or which can compete with the "legacy" system.

To the extent that there is a cohesive "cryptocurrency movement", it is about giving people an alternative, so that they can opt out or route around some problematic issue, like a devaluing national currency or strict capital controls, or refusal for a bank account.

There are many opportunities on this new frontier, there is a lot to be done and there is considerable support (moral and financial) available for the doers. Contributing may mean anything from writing code to providing services to raising awareness of Bitcoin in a particular context.

There is a large and growing number of people who are committed (idealistically and/or financially) to realizing some vision of the crypto commons. To the extent that their visions overlap, they are dedicated to a common cause. On a good day, they recognize and appreciate the others who share this common cause and contribute in a valuable way to realizing their shared objectives.

On a bad day, the proponents of one cryptocurrency may attack projects seen as competitors, and revel in their struggles. There is an element of tribalism to the way that some cryptocurrency proponents and fans contribute to the discourse.

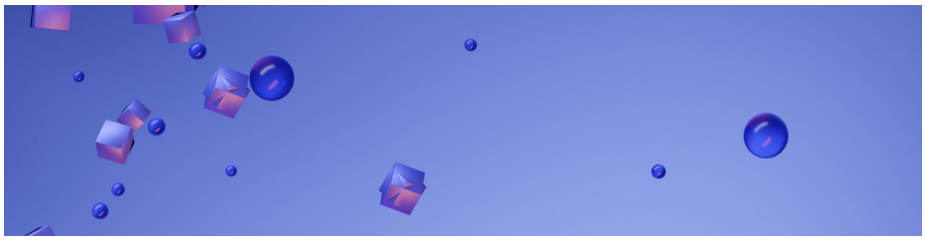
Cryptocurrency projects are all competing with each other across a wide variety of aspects, they can't all succeed in relation to their adoption objectives. One's

desire to see the general movement progress may conflict with a strong preference that one/some asset(s) out-perform their competitors.

References

1. Carter, N. (2018, August 2). *Visions of Bitcoin*. Medium. https://medium.com/@nic___carter/visions-of-bitcoin-4b7b7cbcd24c
2. Carter, N. (2019, February 4). *How to critique Bitcoin: A guide*. Medium. https://medium.com/castle-island-ventures/how-to-critique-bitcoin-a-guide-3e36b26f9642
3. Toby Shorin, Laura Lotti, Sam Hart. (n.d.). *Headless Brands*. https://doi.org/headless-brands
4. Carter, N. (2019, November 3). *A most peaceful revolution*. Medium. https://medium.com/@nic___carter/a-most-peaceful-revolution-8b63b64c203e

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 can 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). If the network does not achieve utility and demand for its native assets, the premine does not reach any significant valuation.

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 [1] $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 precluding 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 and the software required to operate it. In practice, this gives the recipients of ICO funds particular significance in the governance of the network. If the ICO beneficiary decides to change the rules of the network, other constituencies have a choice of either following the party which is endowed to develop the platform (these other constituency members 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

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 [2]. 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.

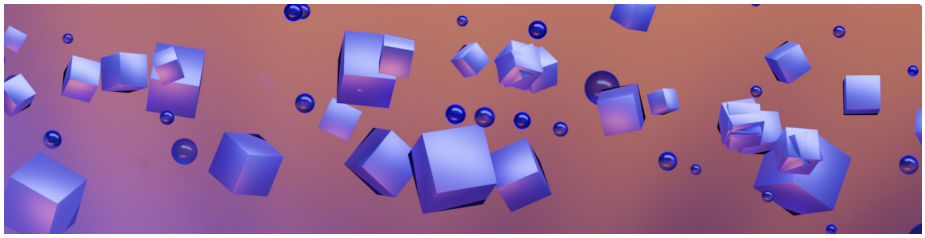
The hard fork was accepted by some participants and rejected by others, with 15% of the mining power sticking to the pre-hard-fork rules [3]. The Ethereum Foundation and founders supported the hard forked chain which re-wrote the blockchain's history, those who refused to consent to the rule change ended 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.

In this case the ICO dynamics left the Ethereum ecosystem in a state where it followed the leaders and ICO beneficiaries, rather than follow the rules of the network and "code is law" principle. The DAO hard fork is revisted in a subsequent section.

References

1. Castor, A. (2018) The Ethereum ICO: Where did all the tokens go? *The Block*. https://www.theblockcrypto.com/daily/5383/the-ethereum-ico-where-did-all-the-tokens-go
2. Ethereum Foundation (2016). *To fork or not to fork*. https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/
3. Ethereum Foundation (2016). *Hard Fork Completed*. https://blog.ethereum.org/2016/07/20/hard-fork-completed/

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 constituents 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 funding and management 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).

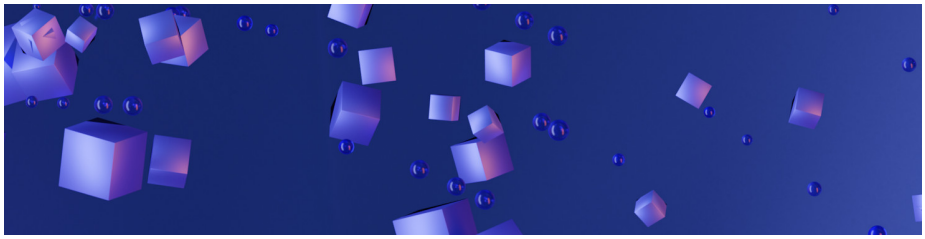
The popularity of "Bounty campaigns" in association with ICOs is an interesting example of the use of open contracts whereby any participants who make certain small measurable contributions (e.g. follow on twitter) are rewarded. Such bounty campaigns are usually geared towards raising the project's profile, 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.

Offering small payments such as bounties to engage contributors on small tasks is quite a transactional approach which is unlikely to bring in contributors who make sustained high quality contributions. A high volume of contributions seeking to collect small bounties can be more effort to manage than it is worth, absent the inflow of the kind of key contributors who make open source projects tick.

Block reward funding can offer stability, regular long-term issuance is an advantage and if the funds are well managed this can create an environment where valued contributors are effectively encouraged to maintain their participation on an ongoing basis. As observations reported in later sections indicate however, there is considerable variation in how well funds created to support blockchain development are spent.

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 harder, better, faster and stronger than other miners.

- PoS is not as 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 double staking 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.
- When a significant amount of an asset is in the custody of an exchange being staked on behalf of its customers - this makes the exchange a potential point of failure.
- With the right smart contract support, people can rent out the voting power of their stake. As with PoW mining hashrate rental markets, whether a chain is exposed depends on the degree to which holders of its asset expose it by making their stake available to rent.

PoS changes the infrastructure surrounding the common pool resource significantly, removing the miner constituency and replacing them with a selection of holders of the asset. 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), and/or locked for some minimum duration.

Delegated Proof of Stake

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 [1] 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.

References:

---

1. Günther, S. (2018, December 11). *Lisk—The mafia blockchain.* Medium. https://medium.com/coinmonks/lisk-the-mafia-blockchain-47248915ae2f

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, storytellers, layer 2 service providers) to play, with the scale and clout of these constituencies varying significantly between projects. Hard fork 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.

From the commons-based perspective of this resource, the most important question is how much of the decision-making process actually occurs on the commons? Where a blockchain's commons are dominated by a small number of entities like corporations or foundations, governance can be dominated by the non-public interactions within and between these entities.

For the portion of a blockchain's governance that occurs on the commons, the key questions are whether and how this is structured. The default, inherited from FOSS, is unstructured rough consensus. This style of unstructured governance has limitations that become apparent when the scale of the endeavour expands or conflicts arise. Jo Freeman's The Tyranny of Structurelessness [1] is highly relevant here, it describes the women's liberation movement in the 1970s, which rejected organizational structure in the same way that blockchain ecosystems reject "centralization". The absence of structure in that case served to empower embedded elites within the movement and restrict the influence of new members as well as the accessibility of the movement.

Successful blockchains are powerful in a way that is new to FOSS software

projects. Unstructured governance may prove to be a weakness, if it allows elites to capture the governance process with behind the scenes machinations.

At the same time, structured governance is not guaranteed to be better for blockchains than unstructured governance. Governance which is structured and developed poorly is probably worse than unstructured governance. The structure is also just the starting point, good governance involves norms and practices that grow with and are reinforced by the community, becoming embedded within their culture.

Commons-based governance of blockchains can happen either "on chain" or "off chain". On chain governance benefits from the same assurances as transactions, immutability and permissionless access being particularly relevant for governance. However, on chain governance can add to the size and complexity of the blockchain, as an additional class of data that must be incorporated.

Dash treasury governance happens largely on chain (submission of proposals, voting on proposals and translating voting outcomes to spending transactions), but the detail of proposals and any discussion around them occurs off chain on other platforms. Decred's consensus rule change governance happens on chain, tickets vote on chain in each block and the results are automatically interpreted and applied by nodes as part of the protocol. Decred also has a significant off chain governance component, with its treasury-related proposals, discussion and voting occurring off chain, although "anchored to" the blockchain in certain ways.

The design of a governance system for a blockchain on paper is difficult to assess, because the degree of fit with the makeup of the stakeholder community and their shared aims is important.

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. The "Crypto Governance Research Project" collects these standard overviews in one place, while the pages about the same projects below in *PPCC* are more about the broader takeaways that we can learn from observing the project.

Before that, I will set the scene by summarizing aspects of Nic Carter's excellent masters dissertation [2], 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

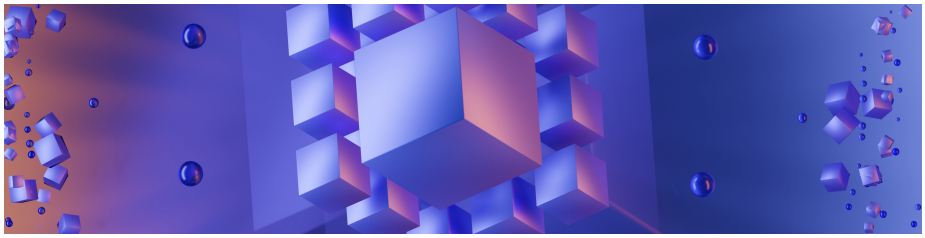
- if governance discourse and decision-making is not observable, participation is not permissionless and the process should therefore be considered as centralized
- to say that a project is "not decentralized" is usually perceived as an attack on that project
- where the major players are centralized 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.

References

---

1. Freeman, J. (1972). *The Tyranny of Stucturelessness*. https://www.jofreeman.com/joreen/tyranny.htm
2. Carter, N. (2017) *A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors*. (2017). /paper/A-Cross-Sectional-Overview-of-Cryptoasset-and-for/deef64a04ae62d307e0dcc87c7f20fa775617cf2

Bitcoin



Bitcoin has featured quite heavily in the previous sections as it is the blockchain with the longest and richest history. This page revisits some of the episodes from the scaling debate in light of the commons based constituencies framing.

- The UASF episode [1] 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 orchestrated 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 [2]. 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 [3] at $1,300 or around 20% of the BTC price).

Skilled Developers Required

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 going forward.

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 [4] 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 last few years have offered much evidence and many demonstrations that maintaining the software for a decentralized cryptocurrency network is not easy. After some catastrophic issues in its early years (like allowing someone to mint billions of BTC) [5], it has been a number of years since any significant exploits have been identified in use on Bitcoin's main chain.

In 2018 a bug was identified [6] by Bitcoin Core developers which would have allowed an attacker to take nodes offline. After a new version of the software had been released and adopted by the majority of miners, it was announced [7] that the bug was actually much more serious than indicated, as it would also have allowed an attacker to print unlimited BTC. The Bitcoin Core developers who patched the bug kept its severity a secret [8] until the patch had been adopted widely enough that the attack would not be able to permeate the network.

There simply cannot be show-stopping bugs that lead to unexpected outcomes in a cryptocurrency's software, or that cryptocurrency will see faith in the solidity of its assets degraded. Respected and skilled developers have power because they are vital to any blockchain, and in short supply.

Is Code Blockchain Law?

In 2010, when an inflation bug was exploited to mint 184 Billion BTC [5], it was spotted immediately and enough miners could be coordinated to effectively roll back the chain. In 2018, there were orders of magnitude more users of Bitcoin, so it is not clear what would have happened if someone had exploited the 2018 vulnerability to mint BTC. If it was not immediately noticed, it is likely that some of the minted BTC could have been sold before anyone realized. A sum like 184 billion BTC stands out quite obviously, but smaller amounts may not be so easily detected.

If Bitcoin was exploited in this way, what would its stakeholders choose to do about it? Discussions about whether the network's peers could or should do anything to mitigate certain kinds of attack/exploit are some of the most interesting ones in the space.

The potential of the social layer to intervene in a crisis by changing the rules is both a defence mechanism or deterrent, and a weakness, from different perspectives.

Bitcoin is software-based, and software is adaptable. For an attacker consider-

ing a major (and likely expensive) attack on Bitcoin, one of the considerations is whether the network's stakeholders will be willing to suffer the damage their attack causes, in order to stick with the rules and the "code is law" principle. With blockchains, there is always the option in principle for the network's stakeholders to rewrite their rules in a way which nullifies or mitigates an attack while maintaining the social contract as they see it. Use of FOSS software means this option is open to any developer who can code it, and from there available to any stakeholder who wants to take it.

The idea of an adaptable blockchain is disagreeable to others, who would tend to see this kind of move as a slippery slope towards stakeholders changing the consensus rules of the network more broadly. Cryptocurrencies are backed by faith that their rules will not change, in particular the idea of a "fixed supply" cryptocurrency rests on the assumption that stakeholders can not or will not change that rule. A cryptocurrency can have a stable monetary policy and predictable supply only in so far as the network's nodes are unwilling to change this - they are always able, if there is collective will.

Mining Dynamics

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.

A 2019 article [9]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.

Developers Have Power

Developer groups must also choose which side of a chain split to join, and for developers this may be a high friction decision, making it difficult to later 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. Surveying the cryptocurrency space as a whole, there are very few blockchains that have seen their founding group of developers displaced by an alternative group. Bytecoin is the only example that springs to mind, where revelations about 80% being secretly premined by its pseudonymous developers led to alternative implementations that surpassed Bytecoin in popularity (Monero being the highest profile).

In 2020, we saw another example [10] of a lead developer team being "outed" from this role, as part of a recent Bitcoin Cash fork. This example is a little different however, in that the developers tried to force a contentious hard fork of which they were the direct beneficiaries - the consensus change would see 8% of block rewards flow to the ABC dev team. This hash war had a clean outcome, although the miner signalling had been divided, and initial hashing was also split, all but a few miners quickly abandoned the ABC chain in favor of the new "BCHN" chain. This sets up an interesting scenario, because the ABC dev team have effectively no working chain using their new client, its block rewards are worth very little at a current price of $15 (Dec 2020) which is ~5% that of BCH(N), the clear winner. The BCH chain has lost most of the developers who worked on its software and miners have shown an unwillingness to fund this work out of block rewards.

The history of most other blockchain projects at this point indicate that developers of pure PoW cryptocurrencies with no formal governance hold the most power within those ecosystems. It remains to be seen what will happen if an issue arises which splits the developer constituency more evenly in two. The level of support from the other constituencies would clearly be important, but so might control of key assets like GitHub repositories. While it may be clear to direct participants that the developer constituency is divided, others may rely on signals like what's happening in the Bitcoin Core repository or what the sticky thread or top post on /r/Bitcoin says.

Chain Splits

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.

Bitcoin has also had a number[11] of "chain split" forks (of the 44 since Bitcoin Cash) where rather than splitting the Bitcoin community the intention is to leverage Bitcoin as an airdrop type distribution method for a new project. Anyone can fork the UTXO set of Bitcoin or any UTXO-based cryptocurrency and award their new coins (which will follow the rules they set) to Bitcoin holders. This seems to have been used as a tactic by some teams for getting a headstart on recognition and awareness - as well as gaming the market capitalization metric with a lot of units that are technically circulating but whose holders are unaware.

Commons-based Deliberation

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 [12] 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, although 2019 meeting logs are harder to find), 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. Miner voting, the only signalling method available to a Bitcoin constituency that's not easily manipulated, has been discounted by most Bitcoin advocates as a legitimate aspect of governance.

As noted in the developers constituency section, Jo Freeman's The Tyranny of Structurelessness [13] is relevant here. Without formal structure to guide decision-making it is likely dominated by the interactions of its elite members, and only

people who are directly involved would be able to follow and understand the dynamics in play.

A 2020 article [14] by Pete Rizzo and Aaron van Wirdum provides a well sourced account of one of Bitcoin's formative governance events following the departure of Satoshi, the "Battle for P2SH". Pay to Script Hash (P2SH) is a way of protecting funds with multi-signature transactions that require multiple private keys to unlock funds. In this episode, a soft fork was seen as an undesirable way to deploy the update because mining power was so centralized that the decision came down to a few pool operators who did not feel qualified to make it or want to have that responsibility. The idea of "miner voting" to choose between two competing multi-sig implementations was considered because it aligned with what was required to activate the changes (hashpower). However, this was rejected due to the precedent it would set, certain developers were keen to avoid the impression that miners were making such a technical decision. Instead, they set up a process where an inner circle would discuss the issue for two weeks and hold a vote. The miners would the be presented with a single option (P2SH) which they would be encouraged to "vote" to activate.

- Additional Resources
  - Jameson Lopp's Bitcoin resources page
  - Hasu's Unpacking Bitcoin's Social Contract
  - Bitcoin Magazine Map of Bitcoin Forks

References

1. Song, J. (2017, August 12). *Bitcoin, UASF and Skin in the Game.* Medium. https://jimmysong.medium.com/bitcoin-uasf-and-skin-in-the-game-7695031c5689

2. Digital Currency Group. (2017, May 25). *Bitcoin Scaling Agreement at Consensus 2017.* Medium. https://dcgco.medium.com/bitcoin-scaling-agreement-at-consensus-2017-133521fe9a77

3. Segwit2x Futures Continue to Trade Despite Fork Cancellation. (2017, November 9). *Bitcoin News.* https://news.bitcoin.com/segwit2x-futures-continue-to-trade-despite-fork-cancellation/

4. Higgins, S. (2017, November 17). *No Fork, No Fire: Segwit2x Nodes Stall Running Abandoned Bitcoin Code.* CoinDesk. https://www.coindesk.com/no-fork-no-fire-segwit2x-nodes-stall-running-abandoned-bitcoin-code

5. Sedgwick, K. (2019, March 1). Bitcoin History Part 10: The 184 Billion BTC Bug *Bitcoin News.* https://news.bitcoin.com/bitcoin-history-part-10-the-184-billion-btc-bug/

6. Hertig, A. (2018, September 19). *Bitcoin Core Developers Move to Fix Denial-of-Service Software Bug.* CoinDesk. https://www.coindesk.com/b

itcoin-core-developers-move-to-fix-denial-of-service-software-bug

7. *CVE-2018-17144 Full Disclosure*. Bitcoin Core. https://bitcoincore.org/en/2018/09/20/notice/
8. *The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret*. (2018, September 21). CoinDesk. https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret
9. Carter, N. (2019, August 5). *It's the settlement assurances, stupid*. Medium. https://medium.com/@nic__carter/its-the-settlement-assurances-stupid-5dcd1c3f4e41
10. Shen, M. (2020, November 15). *Bitcoin Cash Has Split Into Two New Blockchains, Again*. CoinDesk. https://www.coindesk.com/bitcoin-cash-has-split-into-two-new-blockchains-again
11. BitMEX Research. (2018). *List of 44 Bitcoin fork tokens since Bitcoin Cash | BitMEX Blog*. https://blog.bitmex.com/44-bitcoin-fork-coins/
12. Red, R. (2018, April 11). Ch. 5 *A User Perspective and Introduction to Blockchain Governance*. Block Commons. https://www.blockcommons.red/post/user-perspective/
13. Freeman, J. (1972). *The Tyranny of Stucturelessness*. https://www.jofreeman.com/joreen/tyranny.htm
14. Rizzo, P., van Wirdum, A (2020). *How The War For Bitcoin P2SH Was Fought – Bitcoin Magazine*. https://bitcoinmagazine.com/articles/the-battle-for-p2sh-the-untold-story-of-the-first-bitcoin-war

Ethereum

PoW to PoS Consensus

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 the Ethereum proposition. 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.

Technical, Monetary and Political Decisions

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. This introduces significant complexity and the need to ensure that any changes to the rules to allow for upgraded functionality 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 PoS consensus. Switching to PoS would make PoW miners obsolete and remove their constituency entirely from the blockchain's commons. Ethereum's developers have on a number occasions amended [1] 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 December 2018 the Difficulty Bomb went off[1] accidentally.

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 in Feb 2019.

The story of the Difficulty Bomb nicely illustrates a shift in understanding of the power dynamics of changing Ethereum's consensus rules. Its inclusion at Ethereum's launch suggests a view of developers as a relatively weak constituency in comparison to miners. The Difficulty Bomb was included as a check on miners' power, to make it clear that their role was only temporary. By the time it accidentally went off it was obsolete, the developers had already demonstrated their capacity to change the rules, delaying it several times and then agreeing to manually change the issuance schedule directly.

Ethereum's Core developers have also considered [2]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, GPU miners. In 2020,

it the situation came to a head [3] after ProgPoW had been "ninja-approved" on a Core devs call where nobody spoke up against it. This episode also highlighted Ethereum's haphazard governance processes with regard to hard forks.

The DAO hard fork (considered above and below) was a critical moment in Ethereum's governance. It demonstrated the power that the core developers and Ethereum Foundation held. They were able to effectively re-write part of the distributed ledger, in a way that suited themselves (and many other stakeholders) at the expense of another party (the DAO hacker). Despite this being a contentious change, the Core/Foundation were able to retain all of the intellectual property, the brand/name/ticker, and most of the value by market capitalization.

Core developers have since then made a point to emphasize that such rewriting of history will not happen again. As well they might, because belief in the ledger's immutability is a prerequisite for a blockchain to have value.

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 [4] for a fix that would allow these funds to be recovered, and have produced an Ethereum Improvement Proposal [5] 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[5] 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 [6], 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.

Technocratic Council?

Vitalik Buterin[7] and Vlad Zamfir [8] 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 would be excluded from these decisions. However, the same process is followed 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 an 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.

This article [9] by Lane Rettig gives some insight into what it's like to be a participant in Ethereum's governance, through the lens of Ethereum 1.x. Ethereum 1.x is an initiative to improve the current Ethereum blockchain by improving its state management so that it can survive until Ethereum 2.0 is ready, and giving it a chance to thrive long-term.

Some quotes from the article:

> There is growing frustration with how difficult it is to "get anything done" in Ethereum since even seemingly small changes can take months of back-and-forth political wrangling… Coordinating political dialogue among dozens of core developers and attempting to factor in the sentiment of thousands of others in the community, all the while feeling under attack by the media and the public, leads to a lot of stress and enormous cognitive burden.
>
> Ethereum governance today is mostly informal and it happens off-chain in the realm of humans and egos. The EIP process is the one regular, formal governance mechanism, and even *it* is rough around the edges: no one has ever formally defined "core dev" (here's Hudson's most recent takes on this: [one](https://github.com/ethereum/pm/blob/master/All Core Devs Meetings/Meeting 50.md#discussion-about-openness-and-roadmap-discussions-in-prague) two), nor been able to articulate precisely who is invited to the All Core Devs calls nor the precise magic needed to get an EIP brought up in the call. To be clear, I consider this a good thing and one of Ethereum's greatest strengths since a more formalized governance mechanism risks capture, corruption, or losing the discretion of node operators who must proactively opt into forks. However, there is a downside to highly informal governance mechanisms: they tend towards backroom

deals and a lack of transparency.

In Nov 2020 another incident [^10] spotlighted the slapdash approach to consensus rules. A consensus changing update was silently included to address a security vulnerability, most node operators applied this update but not Infura, which provides hosting services for many Ethereum Dapps. When someone else identified the exploit and saw that it was fixed in a recent update, they decided to test it on chain and caused an accidental hard fork which left Infura nodes off the network and many Dapps down. This has prompted further discussions around the process for announcing these changes.

Ethereum's Other Constituencies

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 idea that any faction can exit and fork onto their own chain if they are sufficiently unhappy is embraced as a key principle of Ethereum's governance. In effect this elevates the position of the developers constituency further, because they are probably the key determinants of whether any contentious fork has a realistic chance of surviving and thriving.

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 (Nov 2019 figure) 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 adopting (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.

Ethereum Funding

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.

As part of the Ethereum 1.X initiative, EIP-2025 proposes adding 0.0055 ETH per block to a fund for supporting development of the Eth 1.x chain. 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.

In 2019 the idea of Decentralized Autonomous Organizations (DAOs) has regained popularity in the Ethereum ecosystem, a number of DAOs have been started to administer funding for various activities. These are considered in the DAOs section.

References

1. Kim, C. (2019, February 14). *Ethereum's Blockchain Is Once Again Feeling the 'Difficulty Bomb' Effect*. CoinDesk. https://www.coindesk.com/ethereum-blockchain-feeling-the-difficulty-bomb-effect

2. O'Leary, R.-R. (2019, January 4). *Ethereum Developers Give 'Tentative' Greenlight to ASIC-Blocking Code*. CoinDesk. https://www.coindesk.com/ethereum-developers-give-tentative-greenlight-to-asic-blocking-code

3. Dale, B. (2020, March 5). *Ethereum's ProgPoW Debate Is About Much More Than Mining*. CoinDesk. https://www.coindesk.com/ethereums-progpow-debate-is-about-much-more-than-mining

4. *Parity Urges 'Rescue' Fork to Reclaim Frozen Millions.* (2017, December 11). CoinDesk. https://www.coindesk.com/parity-proposes-hard-fork-to-reclaim-frozen-160-million

5. Harper, C. (2018). *The Evolving Debate Over EIP-999: Can (or Should) Trapped Ether Be Freed?* https://bitcoinmagazine.com/articles/evolving-debate-over-eip-999-can-or-should-trapped-ether-be-freed

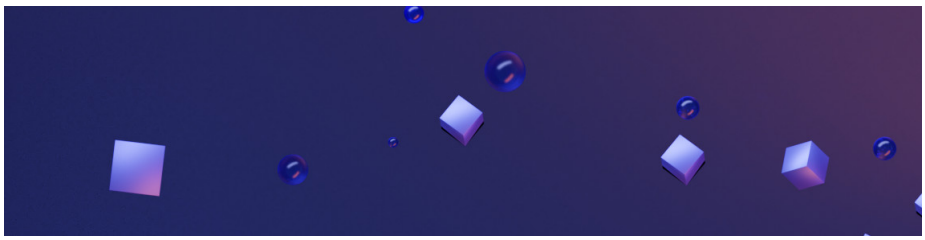
6. O'Leary, R.-R. (2017, November 9). *ICO Funds Among Millions Frozen In Parity Wallets.* CoinDesk. https://www.coindesk.com/ico-funds-among-millions-frozen-parity-wallets

7. Buterin, V. (n.d.). *Governance, Part 2: Plutocracy Is Still Bad.* https://vitalik.ca/general/2018/03/28/plutocracy.html

8. Zamfir, V. (2017, December 3). *Against on-chain governance.* Medium. https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

9. Rettig, L. (2019, January 13). *How open is too open?* Medium. https://medium.com/@lrettig/how-open-is-too-open-bfc412cf0d24

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 [1] has been in deploying the principles of "liberal radicalism" [2], specifically quadratic voting, to fund 25 Ethereum infrastructure projects. This post [3] 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 a greater number of individual donations was taken to mean that more individuals donated to that project, and so it would receive a

larger matching contribution than a project which received a smaller number of large donations. In the first round Gitcoin had $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. Buterin has co-authored a post [4] with the Radical Markets co-author Glen Weyl where Buterin states that he would be interested in applying the concepts to Ethereum.

The report[1] on the initial Gitcoin experiment 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.

Linking human identities to blockchain identities, or ensuring that a single human can only have one identity on chain, is a huge challenge. It could probably only be achieved by heavy reliance on centralized entities, which would then become points of weakness. There are many people who would opt out of or resist any system which attempted to force association between their offline identity and on chain addresses.

A third round of Gitcoin funding with quadratic matching occurred in Oct 2019, and was reported on in detail by Vitalik Buterin [5]. In total $163k was donated to 80 projects by 477 contributors, augmented by a matching pool of $100k.

One of the comments Buterin made was about the relatively low share of funding awarded to Gitcoin itself (it received 0.9% of funding in the round). He praised Gitcoin's efforts and stated that the Ethereum Foundation and Consensys had been giving grants to Gitcoin which included covering some of their running costs.

Vitalik Buterin gives an account [5] of the different projects that were up for donations and where they fit in the Ethereum ecosystem - this kind of context is invaluable for interpreting what the results mean in terms of the effect of voting method. He observed that the grant-giving in this case was less dominated by technical software development proposals, and that QV's effect was to distribute funds in a way which was more aligned with popular opinion in the community.

Buterin's post also explores how a change to the implementation of QV in

round 3 affected the distribution of matching funds. Tweaks to the implementation meant that the presence of any large individual donations would cause the amount of matching funds received to be considerably reduced.

In 2020, Gitcoin continued to thrive, running a further 4 quadratic funding rounds which reached new scale in terms of the level of matching and contributed funding.

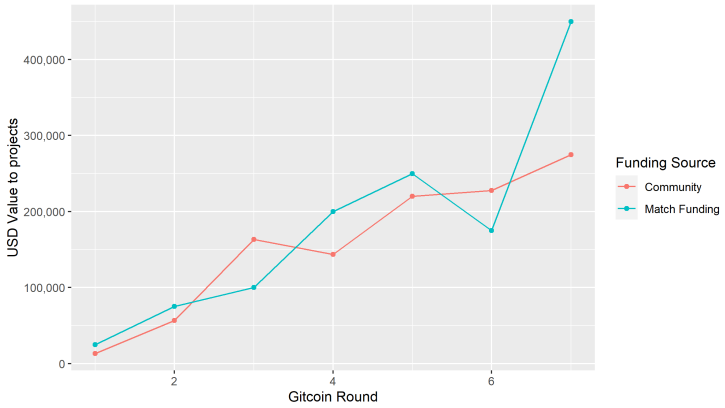


Figure 2: Gitcoin funding per round by source

Gitcoin also expanded its remit by incorporating $100K matching funds for a one-off Public Health fund in round 5 [6], and $50K matching funds for Crypto for Black Lives projects in round 6 [7]. In round 7 the range of funders expanded considerably to include a number of DeFi projects and people, since then Kraken has also joined with $150K of matching funds. This higher level of backing is allowing the Gitcoin team to sustain its ongoing costs of $250K per quarter for development and puts the project on a more secure footing financially. This had previously been an unknown, and Gitcoin co-founder Kevin Owocki opened an EIP (1789) which proposed that inflation funding (20% of issuance) be allocated to Ethereum "ecosystem stewardship". It seems now that the same organizations which provide matching funds are willing to fund Gitcoin's own continued development also.

Gitcoin also extended its scope beyond Ethereum recently with the first Zcash Gitcoin Grants [8] round, where $25K matching funds were distributed on the basis of 156 donations totalling $2,137. This was the first Gitcoin grant round on a UTXO chain and furthermore many Zcash users expressed a desire to be able to use shielded transactions to donate/receive, which were not supported for this initial round.

The major controversy around Gitcoin in 2020 concerned the share of funding which was going to popular social media personalities in the Ecosystem, specifically This was addressed by Vitalik Buterin in his results commentary post for

round 4 [9]. @antiprosynth is a twitter account that tweets pro-Ethereum messaging and information, and was at one point on course to be the largest beneficiary in a new "Media" category and receive a ~$20K match in funding, which caused some discussion of whether this was too much for tweeting or whether tweeting was even a public good. By the end antiprosynth's matching amount had reduced to $11,316 after a kind of campaign to increase contributions to causes deemed more worthy had seen a couple of those overtake it.

Gitcoin is meeting a need in the Ethereum ecosystem, as evidenced by the funding which major institutions like the Ethereum Foundation have poured into it. It is an interesting experiment in quadratic funding, which encourages smaller stakeholders to participate by matching their contribution with a relatively larger share than those who donate a lot. The major problem with applying quadratic funding in the crypto space is that it's usually easy for a motivated actor to cheat by creating multiple accounts and spreading their funds out that way, to avoid the penalty imposed on larger contributors by appearing as many smaller contributors to get the benefits which these participants receive. This is the same issue which limits the utility of open decentralized systems which are "one person one vote", it doesn't work because people can create as many "persons" as they want, unless there is some central authority to decide what counts as a person (in this case the Gitcoin team).

There have indeed been some issues with gaming the system as recounted in Vitalik's blog posts, and as a way to compensate there are now a series of methods through which a funder can enhance their matching level or "Trust Bonus". I haven't looked into the privacy implications of completing any or a number of these and associating that identifying information with one's Ethereum account address, but I hope the people who get the "Trust Bonus" have done their research and that they're not trusting Gitcoin with too much sensitive info.

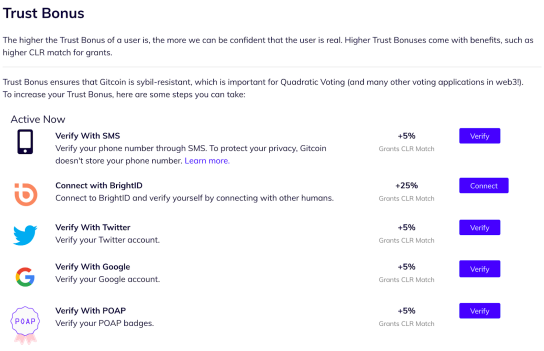


Figure 3: Gitcoin Trust Bonus

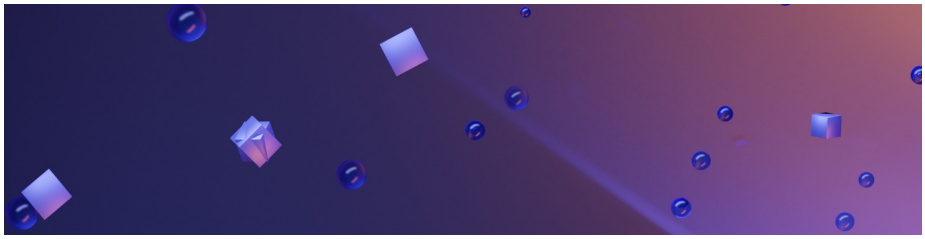
Gitcoin and the "RadicalxChange movement" [10] is a good example of experimentation with new funding and economic models in the blockchain context.

Blockchains would appear to be ideal laboratories for experimentation with approaches to governance and economics. They have the capacity to apply rules rigidly, they're as flexible as software and they have all the problems of an emerging technology and mode of production to solve.

References

1. Singh, V. (2019, February 22). Radical Results: Gitcoin's $25K Match. *Gitcoin's Blog*. https://gitcoin.co/blog/radical-results-gitcoins-25k-match/
2. Buterin, V., Hitzig, Z., & Weyl, E. G. (2018). *Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds* (SSRN Scholarly Paper ID 3243656). Social Science Research Network. https://doi.org/10.2139/ssrn.3243656
3. Singh, V. (2019, June 12). *Experiments With Liberal Radicalism*. Medium. https://medium.com/gitcoin/experiments-with-liberal-radicalism-ad68e02efd4
4. Buterin, V. & Weyl, G. (2018, May 21). *Liberation Through Radical Decentralization*. Medium. https://medium.com/@VitalikButerin/liberation-through-radical-decentralization-22fc4bedc2ac
5. Buterin, V. (2019). *Review of Gitcoin Quadratic Funding Round 3*. https://vitalik.ca/general/2019/10/24/gitcoin.html
6. Singh, V. (2020, March 23). Gitcoin Grants Round 5: Funding Our Future. *Gitcoin's Blog*. https://gitcoin.co/blog/gitcoin-grants-round-5-funding-our-future/
7. Buterin, V. (2020). *Gitcoin Grants Round 6 Retrospective*. https://vitalik.ca/general/2020/07/22/round6.html
8. Owocki, K. (2020, December 3) Zcash Gitcoin Grants round 1 retrospective. *Electric Coin Company*. https://electriccoin.co/blog/zcash-gitcoin-grants-round-1-retrospective/
9. Buterin, V. (2020). *Review of Gitcoin Quadratic Funding Round 4*. https://vitalik.ca/general/2020/01/28/round4.html
10. Kim, C. (2019, March 26). *The RadicalxChange Movement's Crypto-Cypherpunk Appeal*. CoinDesk. https://www.coindesk.com/understanding-the-radicalxchange-movement-and-its-cypherpunk-appeal

Monero



Rough Consensus Hard Forks

Monero is a privacy-focused PoW cryptocurrency with rough consensus governance that makes regular hard fork upgrades. These hard fork upgrades include technical advances (like bulletproofs [1], 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 incompatible. 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 (see PoW miners section) 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 with the change to consensus rules lost most of their utility and would become significantly less valuable).

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.

Community Crowdfunding System

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.

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.

Income Security

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 debate about Zcash funding (see Zcash section), 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.

Income security or reliability is likely an important component of a software developer's decision-making about whether to spend some of their working time, and how much, on commons-based resources. Zcash has a stronger offer in terms of funding security, and probably also larger amounts available to individuals. On the other hand, Monero developers are more directly engaged with and supported by the broader ecosystem, and this is likely to enhance their intrinsic motivation.

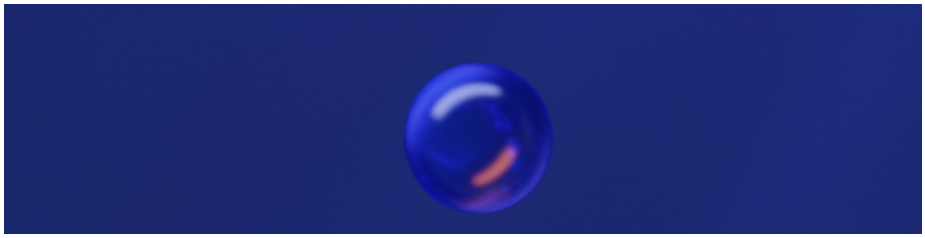
Software engineering is typically not a domain where it is productive to try and boost progress with an influx of capital and new hires. "The Mythical Man-Month" is a well known book which describes the phenomenon whereby adding extra staff to a software project can actually slow it down, due to the costs associated with productively onboarding new members to a team. It is desirable to attract and retain committed engineers. The amount of funding available matters, but so too do the working conditions and perceived security of the income source.

References

1. O'Leary, R.-R. (2018, October 17). *Monero to Become First Billion-Dollar Crypto to Implement 'Bulletproofs' Tech.* CoinDesk. https://www.coin

desk.com/monero-to-become-first-billion-dollar-crypto-to-implement-bulletproofs-tech

EOS



DPoS Consensus, ICO to distribute tokens

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 [1].

The EOS mainnet launched in June 2019, after a few false starts and generally hard time[2], with security issues uncovered by audits and phishing attacks on Block.one's email address book.

Block Producers

The best resources I have found which describes the BPs and how they are rewarded are this infographic[3] by Steve Floyd and this FAQ[4] 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 at Aug 2019 prices - 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.

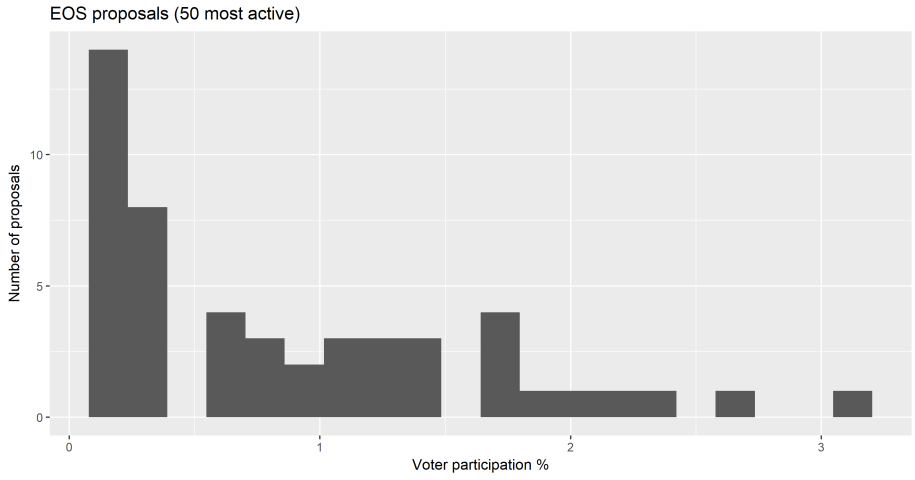
An example of this occurred shortly after EOS launch in June 2018, when the EOS Core Arbitration Forum (ECAF) responded to complaints of private keys being stolen by ordering BPs to freeze 27 accounts[5]. The BPs coordinated to freeze these accounts by agreeing not to process transactions from them, 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 [6].

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.

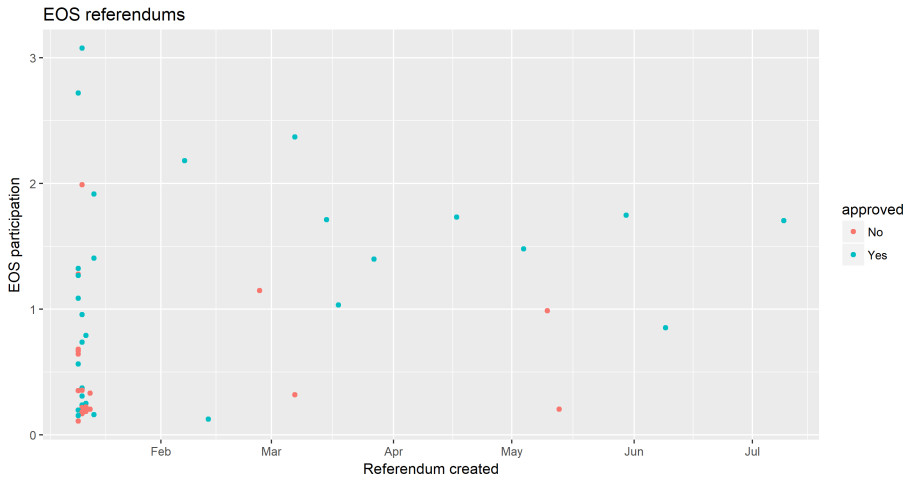
Referendums

EOS referendums went live in January 2019 [7], 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.

Block Producers Change the Rules

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 ap-

proved, 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.

BPs and Whales

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 EOS Commons

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 and paid for 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.

With the domination of the EOS commons by large holders such as Block.one, Bitfinex and Huobi, it is not surprising that the token distribution is the main aspect which has been changed [8] in an alternative network running EOSIO software, Telos. Telos was formed by EOS community members who were displeased with the way EOS mainnet was going, and while the distribution retains some basis in the ICO sale, individual allocations have been capped so that the largest contributors miss out on most of their share of tokens. Telos is only listed on one small exchange with a market capitalization of just $3.4M (Dec 2020), but it seems to have an active BP community (with the 21 active BPs earning ~$1,000 per month).

After Block.one was ordered to pay $24 million to the SEC [9] for running the EOS ICO, it is possible that Telos is suffering from the association. For Block.one this was an almost insignificant sum, easily covered by ICO profits and less than they paid for the voice.com domain [10]- for a new social network that later decided not to use EOS.

Around the time that the initial version of *PPCC* was released, EOS entered

"congestion mode"[11], which raised the threshold for making transactions and left many users unable to move their funds or use the blockchain. The issue was caused by a useless airdrop[12], EIDOS, whose purpose was to encourage many transactions and clog up the EOS chain to make a point about BPs and the network. This congestion persisted for weeks [13], resulting in issues with the Resource Exchange (REX) which users must navigate to lease the resources needed by Dapps.

While things have been going wrong on the EOS commons, Block.one have been doing quite well, paying out returns of up to 6,567%[14] to some early investors, and holding a reported 140,000 BTC on its balance sheet.

References

1. Suberg, W. (2018). *EOS About to Secure a Record $4 Bln in Year-Long ICO*. Cointelegraph. https://cointelegraph.com/news/eos-about-to-secure-a-record-4-bln-in-year-long-ico

2. Varshney, N. (2018, June 8). *The EOS mainnet nightmare: How not to launch a blockchain network*. Hard Fork | The Next Web. https://thenextweb.com/hardfork/2018/06/08/eos-mainnet-nightmare/

3. Floyd, S. (2018, May 22). *How EOS Block Producers are Paid*. Medium. https://medium.com/eostribe/how-eos-block-producers-are-paid-7b2a1216eb2b

4. Sigman, B. (2018). *EOS Block Producer FAQ. The EOS launch is less than 1 month… | by Ben Sigman | Medium*. https://medium.com/@bensig/eos-block-producer-faq-8ba0299c2896

5. Floyd, D. (2018, June 22). *EOS' Blockchain Arbitrator Orders Freeze of 27 Accounts*. CoinDesk. https://www.coindesk.com/eos-blockchain-arbitrator-orders-freeze-of-27-accounts

6. *Proposed Solution For a Broken Blacklist | by EOS42 | Medium*. (n.d.). https://medium.com/@eos42/proposed-solution-for-a-broken-blacklist-ce1c18bdf81c

7. HKEOS. (2019, March 15). *What You Missed in EOS | 1.7.2019–1.20.2019*. Medium. https://medium.com/hkeos/what-you-missed-in-eos-1-7-2019-1-20-2019-3ab666d4eb01

8. Vancouver, E. O. S. (2018, July 12). *Telos Network launches first sustainably decentralized EOSIO-based blockchain*. Medium. https://medium.com/@eosvancouver/telos-network-launches-first-sustainably-decentralized-eosio-based-blockchain-b15d98bb0d52

9. *SEC.gov | SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO*. (2019). https://www.sec.gov/news/press-release/

2019-202

10. Biggs, J. (2019, June 19). *Block.one Paid $30 Million for a Domain*. CoinDesk. https://www.coindesk.com/block-one-pays-30-million-for-a-domain-name

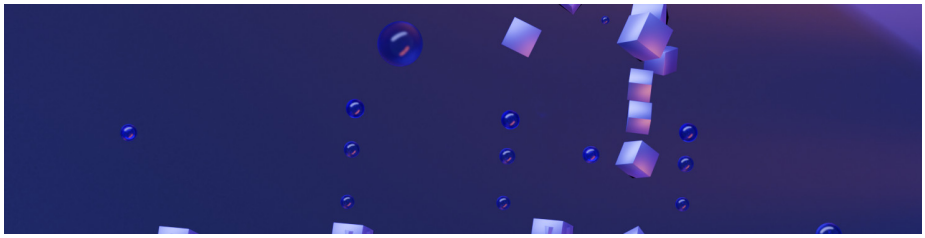
11. Coinbase. (2019, November 9). *EOS enters congestion mode due to EIDOS airdrop*. Medium. https://blog.coinbase.com/eos-enters-congestion-mode-due-to-eidos-airdrop-3d3f82081074

12. Dale, B. (2019, November 11). *A Mysterious Airdrop Called EIDOS Is Clogging EOS to Make a Point*. CoinDesk. https://www.coindesk.com/a-mysterious-airdrop-called-eidos-is-clogging-eos-to-make-a-point

13. Dalton, M. (2019, November 28). EOS's Dan Larimer Has Plans To Reduce Network Congestion. *Crypto Briefing*. https://cryptobriefing.com/dan-larimer-has-proposed-a-new-resource-allocation-model-that-will-combat-network-congestion-on-eos/

14. Marsh, A. (2019). *Peter Thiel Startup Block.One Pays Out 6,567% Investor Return—Bloomberg*. https://www.bloomberg.com/news/articles/2019-05-22/thiel-backed-crypto-startup-pays-out-6-567-return

Tezos



Baking Consensus

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 (writing in Sep 2019 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.

Development Funding

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.

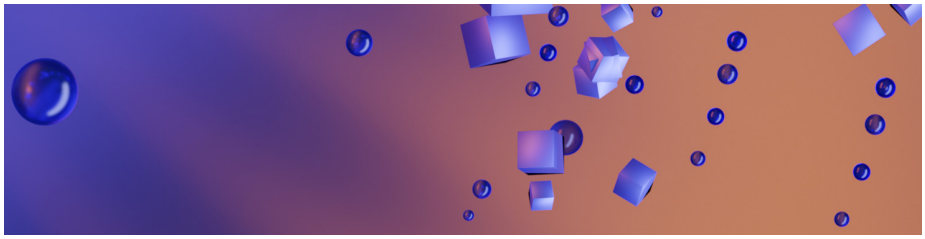
A report published in Aug 2019 provides some insight into how the Tezos Foundation is managing its funds. They hold 61% of their $650 million USD equivalent as BTC, 15% as bonds/etfs/commodities, 15% as XTZ (their ICO tokens and staking rewards, untouched), 6% fiat. The Foundation funds a large number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

Decred defines a constituency of stakeholders that have collective responsibility for governing the network, and embeds mechanisms through which this constituency can make and implement decisions. Holders of DCR (Decred's native asset) can time-lock it in exchange for tickets, and voting with these tickets is integral to block production and decision-making. The rationale is that people with locked DCR balances have skin in the game and are incentivized to look out for the network's best interests.

Consensus PoW miners compete to solve random puzzles and create new blocks, providing security for the network and collecting 60% of the Deced 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, but miners don't get their full reward unless all 5 tickets vote. 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 more robust to majority attacks [1] than a PoW network with equivalent security spend. 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 [2]. 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. In a network with pure PoW consensus, nodes willingly abandon their view of the blockchain's state when presented with a longer Proof of Work chain. Staking Decred nodes have weight on the network, they approve every block and will not vote on blocks that would cause a significant reorg, giving them the collective power to reject such attempts.

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, towards 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 Treasury funds is deliberately loose, confined to signalling approval or rejection of proposed spending (and in the future approving each aggregated monthly spend). Proposals which are intended to dictate how contributors (e.g. wallet developers) approach their work are not allowed. Anyone who a proposal relies on must be voluntarily on board for it to be valid.

This approach is intended to preserve the autonomy of contributors and create a good working environment and incentive 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. Individuals may also approach the stakeholders directly to seek approval for funding of their work, by submitting a proposal. The conventional approach of receiving applications and conducting interviews is eschewed in favour of demonstrated ability to make valued contributions.

There is 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[3]. 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 compensate contributors to the various FOSS projects that make up the Decred ecosystem. The open source ethos runs deep within the project, as reflected in the project's constitution.

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.

Politeia Politeia is an off chain governance platform (modelled on reddit) where proposals can be submitted and discussed in an environment with accountable censorship, and 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 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. A number of the project's lead developers work for Company 0, but over time the proportion of work being done by other

contractors has steadily increased, and Company 0 are now in the minority.

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, with the aim of learning from their 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 Telegram, 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.

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).

Delegation

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 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.

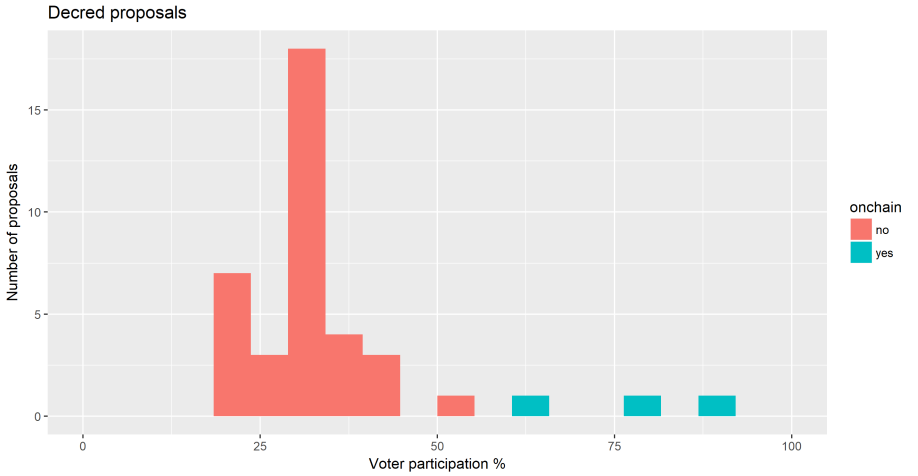
Commons-based decision-making

Participation in Decred's Proof of Stake component is relatively high, with around 50% of circulating DCR being time-locked in exchange for tickets at any given time circa mid-2019. Half of all the circulating DCR is represented by live tickets.

Starting in May 2017 , 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.

On Politeia, proposals that pass admin review 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.

Politeia launched on Oct 16 2018, and after one year of operation [4] 53 proposals had been published, 38 proceeded to a vote, with 25 approved and 13 rejections. Of the tickets that were eligible to vote on each proposal, there was a mean turnout of 31%. In the second year of Politeia's operation [5], there were 46 proposals and mean ticket turnout was 28%.

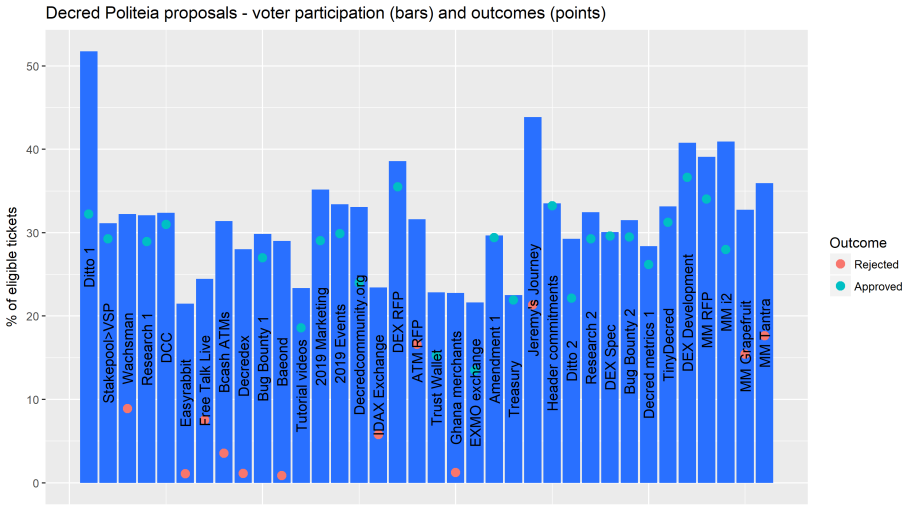


Proposals have been approved which cover decisions like hiring a PR firm, approving a marketing budget, various research projects, DEX infrastructure,

Python tools, a bug bounty, and policy decisions like a new contractor clearance process and an amendment of the project's constitution.

The Decentralized Exchange (DEX) infrastructure proposals are interesting because they cross the boundary between cryptocurrency and DEX projects. The Decred community were not happy with the influence that centralized exchanges had on the cryptocurrency space, or with what other DEX projects had to offer (these usually introduce a token and charge fees so that the token has a purpose). Stakeholders voted to commission FOSS that would allow anyone to run a non-custodial client-server DEX based on atomic swaps and with a number of features to combat things like order spoofing and front-running.

In Oct 2020 the initial DCRDEX MVP was released [6], enabling users of the Bitcoin and Decred command line interface wallets to connect to a DCRDEX server and allow it to coordinate atomic swap transactions to execute trades.



I wrote about the first year of Politeia in a blog post](https://blockcommons.red/post/year-of-politeia/) [7]. One of the stand-out trends was the degree to which the stakeholders approved proposals from people who were established contributors to the project, many of these achieving 90% or greater approval. The most controversial proposals were those which were competing directly against other proposals. A Request for Proposals type process was used to solicit competing proposals for the provision of public relations and market making services. In 2020, a formal RFP type of proposal was added to Politeia, this first seeks approval for a round of tendering proposals, which are then pitted against each other in a run-off vote.

Once Politeia proposals are approved, this is a green light for work to proceed and the worker(s) to bill according to the agreed schedule/rate as they complete it.

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.

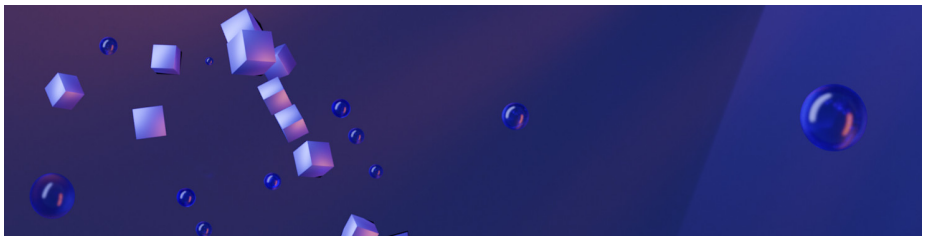
References

1. Zia, Z. (2019, April 3). *Decred's hybrid protocol, a superior deterrent to majority attacks*. Medium. https://medium.com/decred/decreds-hybrid-protocol-a-superior-deterrent-to-majority-attacks-9421bf486292
2. Red, R. (2019, January 25). *The role of Decred voters in defending against majority attacks*. Medium. https://richardred.medium.com/the-role-of-decred-voters-in-defending-against-majority-attacks-ec658af0a8fd
3. Yocom-Piatt, J. (2015). *Bitcoin's biggest challenges | Company 0*.https://blog.companyzero.com/2015/11/bitcoins-biggest-challenges/
4. Red, R. (2019, October 16). *One year of Decred's Politeia in numbers and graphs*. Block Commons. https://www.blockcommons.red/publication/politeia-at-1/
5. Red, R. (2020, October 16). *Year two of Decred's Politeia in numbers and graphs*. Block Commons. https://www.blockcommons.red/publication/politeia-at-2/

6. Mollen, F. (2020, October 21). Decred Announces its First Zero-Fees Decentralized Exchange: DCRDEX. *CryptoPotato*. https://cryptopotato.com/decred-announces-dcrdex-decentralized-exchange/

7. Red, R. (2019, October 22). *The First Year of Decred's Politeia*. Block Commons. https://www.blockcommons.red/post/year-of-politeia/

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 master nodes (there are many projects which have emulated the master node concept) [1]. 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"[2] 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 master nodes 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 - although in 2020 this is changing, see bottom of page.

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 (~$500 at Dec 2020 prices) 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 block the votes are tallied. The proposals are ranked and an eligibility criteria applied. To be eligible to receive funds proposals must have 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 [3]. The second about the various support structures surrounding it [4], 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

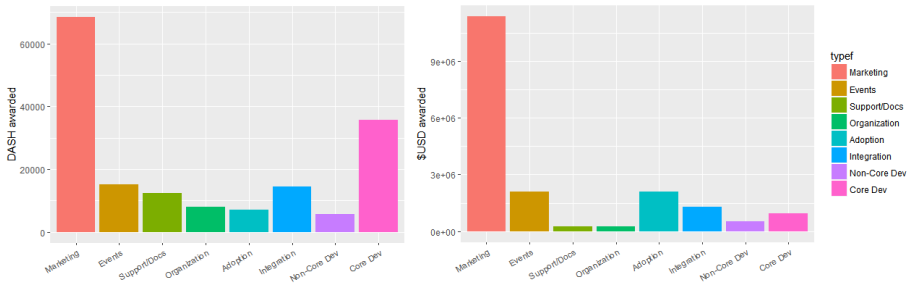


Figure 4: Dash Treasury Spending from Aug 2015 to Jan 2018

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[5] 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 PoW miners and master nodes always go along with these decisions by updating their software, so far at least.

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 [6], 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. Dash Evolution is a major update which has been in the works for years [7], announced initially in 2016 then expanded in scope, but as yet unreleased. The level of communication on Evolution between DCG and the rest of the Dash ecosystem has not been high, and the term even disappeared from the dash.org website. Some prominent community members have expressed disappointment about the rate of progress towards Evolution, but as the internal workings of DCG are largely unknown to the rest of the Dash community it is difficult for them to know whether an intervention is warranted.

In Dec 2019, after the release of *PPCC*, Dash Evolution was formally abandoned, referred to in the past tense by an open house roadmap presentation which instead featured "Dash Platform" in its place.[8]

Dash's 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.

In 2020 we saw an example of the Master Node Operators putting in a counter-proposal against one from DCG, although it was beaten by the DCG proposal in a head to head. See below.

Commons-based Decision-making

Dash Treasury proposals are submitted and voted on the blockchain itself, so this aspect of decision-making happens on the commons, and the commons have been furnished with the tools to also put those decisions into practice (i.e. payments are made automatically based on voting outcomes).

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 [9], 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 [10], 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.

There seems to have been some friction between the Dash Investment Foundation (DIF) and the MNs, with the DIF board putting out a statement to address some friction (rejected proposals and private criticism from master nodes) and

announcing that it will no longer seek decision-making autonomy and will reduce its ask from the Dash Treasury, coming up with a new VC strategy during Q2 2020. In Dec 2020 the DIF published a blog post about a change of process, explaining that due to the sensitive nature of investment details these could not be shared with the MNs publicly, and this meant that it would not be possible to have MNs vote to approve each decision after all. The DIF would have to take autonomous decisions and the MNs can stop funding them or elect new Directors if they don't like it.

Elections have become a feature of Dash governance in recent years, with electing representatives to Dash Trust (which can change DCG Directors) and Dash Investment Foundation established as ongoing practices.

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 4,800 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% [11].

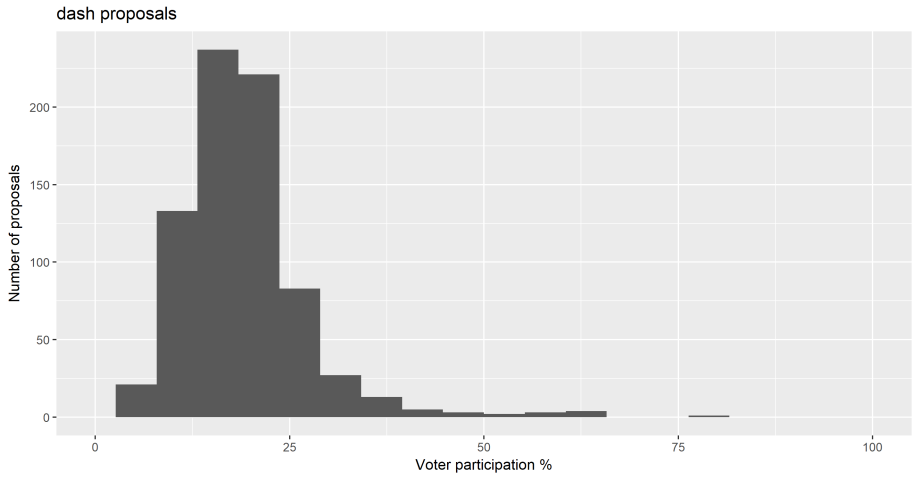


Figure 5: Dash proposals master node voting Apr 2015 - Apr 2019

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.

2020 Updates

In 2020 Dash is making major changes to its network, primarily on the development funding and economics side, in response to weak market performance.

Ryan Taylor had previously suggested [12] that a block reward reallocation proposal was coming, and in June a Dash Core Group presentation [13] was livestreamed, in which he and others set out analysis of Dash Economics which suggested reducing miner rewards and giving more of these to the Master Nodes. I'm not a big fan of 2.5 hour videos as the main place where one describes this kind of fundamental change to the network, I watched it once and made some notes but I'm not going back in to check details in a video that runs 150 minutes long.

The first written version seems to be courtesy of Luxor mining pool, but the proposal on Dash Central also has a written description, from Ryan Taylor. The plan is to increase the Master Node share by reducing the Miner's share, such that they go from enjoying a 50/50 split, to a 60/40 split in favor of MNs. The background to the proposal suggests that with Chainlocks in place now the MNs don't need the miners as much to secure the network, so it suggests using some of that DASH to incentivize locking up DASH for MNs, and thereby boosting the price of the asset by stimulating demand and decreasing the amount which miners have to sell. MNs voted to approve this change by 1,152 yes votes top 91 no votes - so participation of about 25% of MNs.

There's an argument to be made that once you change the issuance schedule

you have weakened the social guarantees around things like fixed supply, by showing that details can be changed by certain constituencies. In Dash's case this is the latest of many amendments, as it has been changing its issuance schedule since correcting the "instamine" bug, reducing the maximum supply as Xcoin/Darkcoin and adding MasterNodes as major beneficiaries of the block rewards.

Following the activation of the block reward changes transition period ion September, attention shifted to the Dash Treasury proposal system and two proposals were pitted directly against each other, one from the Dash Core Group and one from a group of master nodes. Both proposals expand the maximum possible share of the block reward which proposals can receive from 10% to 20%, and make this more flexible by removing the rule that burns unspent funds, allowing these to be collected by MNs and miners along with the other 80%. The difference between the two proposals comes down to the MN proposal giving all the unspent DASH to the MNs, whereas the DCG proposal would share these "rebates" with miners. The DCG proposal won the head to head round and is on its way to being enacted.

The proposal from the MNs referenced a poll by Ryan Taylor on Discord which asked questions about a few options for reallocating the block reward between miners/MNOs/Treasury - this seems to have been influential in forming the proposals. Many projects have channels or rooms on some platform where community members discuss topics, and these can be quite influential on the course the community takes if key members are present and engaged.

References

1. https://masternodes.online/ keeps a table of blockchains that use Master Nodes
2. Block, A. (2019, October 23). *Mitigating 51% attacks with LLMQ-based ChainLocks*. Medium. https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9
3. Red, R. (2018, May 16). *Observations of the Dash Treasury DAO*. Block Commons. https://www.blockcommons.red/post/dash-treasury/
4. Red, R. (2018, September 4). *Decentralized Autonomous Funding of Blockchain Projects*. Block Commons. https://www.blockcommons.red/post/decentralized-autonomous-funding/
5. Dash Watch has been funded since November 2017 to keep track of Treasury funded proposals, seeking information from the people operating those proposals on a regular basis and turning this into reports which assess whether milestones are being met.

6. Valenzuela, J. (2018). *Dash Core Group Becomes First Legally DAO-Owned Entity | Dash News*. https://dashnews.org/dash-core-group-becomes-first-legally-dao-owned-entity/

7. *Dash (DASH): Dash Evolution Platform Update To Roll Out In Q4 2018*. (2018, August 14). Crypto Daily Gazette. https://cryptodailygazette.com/2018/08/14/dash-dash-dash-evolution-platform-update-to-roll-out/

8. Gutierrez, F. (2019, December 10). *Dash Evolution Open House Recap*. Medium. https://blog.dash.org/dash-evolution-open-house-recap-cfcdc1e5abd9

9. *Dash Launches Dash Investment Foundation To Expand Growth Opportunities | Dash News*. (2019). https://dashnews.org/dash-launches-dash-investment-foundation-to-expand-growth-opportunities/

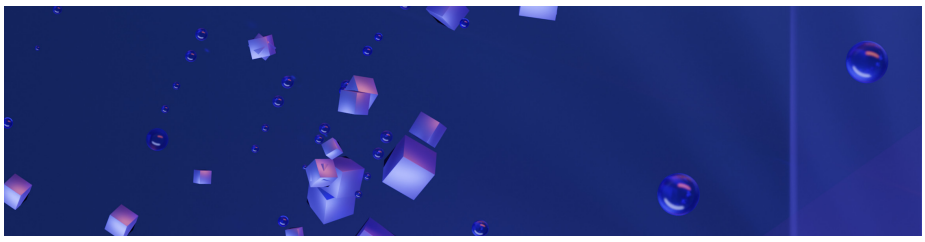
10. *Dash Investment Foundation Enables More Expansive Network Investments | Dash News*. (2019). https://dashnews.org/dash-investment-foundation-enable-more-expansive-network-investments/

11. Crypto Governance Research Overviews (2019, December 9). *Dash*. Block Commons. https://www.blockcommons.red/crypto-governance-research/overviews/dash/

12. Dash - Digital Cash. (2019, December 11). *Ryan Taylor—Improving Dash As A Store Of Value*. https://www.youtube.com/watch?v=7yylT6gAihc

13. Dash - Digital Cash. (2020, June 4). *Dash Core Group Presentation on Dash Economics*. https://www.youtube.com/watch?v=hUf76R2V3pY

Zcash



Zcash relies on pure PoW consensus and is mined by ASICs. Having formerly considered itself "ASIC resistant", it made no moves [1] 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"[2] 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 was 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.

Whether and How to Replace Block Reward Funding

This section was written in 2019, there follows an update at the bottom with the conclusion of the saga.

The attention of the Zcash ecosystem in 2019 turned towards sustaining development beyond the duration of the founders' reward [3], with Zooko expressing support for a continuation of block reward funding[4] 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 many ICO funded projects each 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[5] 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.[6] 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 Electric Coin Company

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 [7] 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 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

The Zcash Foundation has a mandate to represent the Zcash stakeholder community, and ample funding sourced originally from Zooko Wilcox's share of the founders reward. This blog post [8] 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 subse-

> quent 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.

At time of writing in 2019 Zcash had yet to detail how the decision about future funding will be made, but according to this megathread it would involve some form of polling and then a 2-of-2 decision from ECC and ZF about which consensus rule change to move forward with, if any. As an external observer, one of the most salient points for me has been how difficult it is to follow the discussion around this subject, as it is divided between a number of different platforms, forum, twitter, blogs/announcements.

The conclusion of the funding debate - round 1

In November 2019, the Zcash Foundation and ECC reached agreement [8] on how to handle the Zcash trademark. This has been transferred to the Foundation, with an agreement where it shares bilateral power to enforce the mark with ECC. This article[9] gives an account of the dispute as about more than a logo, bringing in the power of the trademark holder to effectively decide which chain is Zcash.

The resolution of the trademark dispute meant the "Zcash Dev Fund Community Sentiment Collection Poll" could begin. This was comprised of a poll for members of the Community Governance Panel, a poll for Zcash Community Forum users with accounts older than a certain date, and a poll for miners who could signal with hashpower. There were 13 proposals to choose from in the polls, most originating in forum posts and then being refined. Voters could signal support for all 13 proposals by voting Yes/No on each one.

In December 2019, the results of the Zcash community sentiment polling were released. Participants were the community advisory panel and forum users, none of the PoW miners chose to signal using the polling method offered to them. There was also an unofficial coin vote which had limited participation (~1%), possibly because participation had privacy drawbacks. No miners repsonded to the

There was very little support for proposals that did not continue to dedicate 20% of the block reward to development funding.

48 of the 62 Community Advisory Panel members responded to the poll, as did 77 forum users (of 104 eligible). The most popular options had continued funding for ECC and Zcash Foundation (it's unknown how many voters were employees of one of these organizations).

The Zcash Foundation decided to develop option #12 with some improvements, then rolled back on most of the improvements in response to pushback. Following some more negotiations ZIP 1014 was revealed for community sentiment collection. ZIP 1014 extends the block reward for 4 years at 20%, with 35% going to ECC, 25% to Zfnd, and 40% for additional "Major Grants". Changes to the proposal involve making it more directly controlled by Zfnd, and removing a restriction that would have excluded ECC from receiving any funding as part of "major grants", and later removing a USD cap on ECC's earnings. Another change added to the proposal by Zfnd is to "Call for, and incentivize, development of decentralized voting and governance".

The solution found for Zcash dev funding is a temporary one, and at the end of the next epoch the question will be raised again. Although the ECC and Zcash Foundation are the only entities with any real power (you could add the miners to that list possibly if they had shown any interest in the process), it still took almost a year of on/off discussions that occupied many community members' time to resolve this time around.

A few months after ZIP 1014 had finally been agreen on, Josh Cincinnati resigned as the Executive Director of Zcash Foundation, citing a number of reasons, including the loss of trust with the ECC and damage to their working relationship following the trademark dispute.

References

1. *Zcash Exercises Restraint as the Antminer Z11 Release Approaches.* (2019). Cointelegraph. https://cointelegraph.com/news/zcash-exercises-restraint-as-the-antminer-z11-release-approaches

2. Funding, Incentives, and Governance. (2016, February 1). *Electric Coin Company.* https://electriccoin.co/zh/blog/funding/

3. Copeland, T. (2019). *Zooko Wilcox gives the Zcash community an ultimatum.* https://finance.yahoo.com/news/zooko-wilcox-gives-zcash-community-154140125.html

4. Wilcox, Z. (2019, August 4). *A Personal Letter About The Possibility of a New Zcash Dev Fund.* Medium. https://medium.com/@zooko_25893/a-personal-letter-about-the-possibility-of-a-new-zcash-dev-fund-f6d30df64392

5. Beedham, M. (2019, July 25). *TRON's Justin Sun confirms he's a 'big-mouthed over-marketer' in Warren Buffett lunch apology.* Hard Fork | The Next Web. https://thenextweb.com/hardfork/2019/07/25/justin-sun-tron-marketing-buffett-lunch-cancelled/

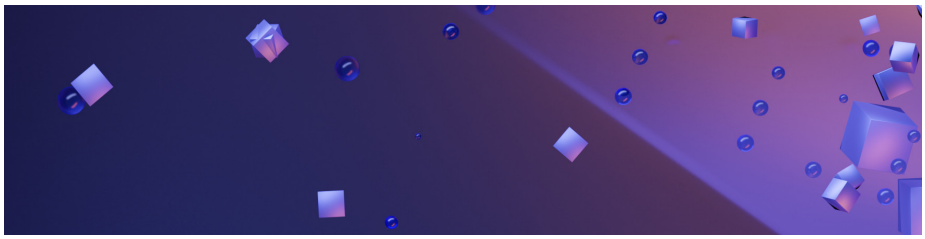
6. *Parity teams up with Zcash Foundation for Parity Zcash client.* (2018, October 30). Blockchain Infrastructure for the Decentralised Web. https://www.parity.io/parity-teams-up-with-zcash-foundation-for-parity-zcash-client/

7. Zcash Counterfeiting Vulnerability Successfully Remediated. (2019, February 5). *Electric Coin Company.* https://electriccoin.co/blog/zcash-counterfeiting-vulnerability-successfully-remediated/

8. Cincinnati, J. (2019). *A Solid Future for the Zcash Trademark.* The Zcash Foundation. https://www.zfnd.org/blog/zcash-trademark-resolution/

9. Cuen. (2019, November 7). *Zcash Trademark Talks Were About More Than a Logo.* CoinDesk. https://www.coindesk.com/zcash-trademark-talks-were-about-more-than-a-logo

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 weaknesses or forms of attack from this.

Blockchains excel at imposing rules on participants' actions, they are excellent bureaucracies [1]. 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 examples of DAO instances which use them.

References

---

1. Laul, M. (2019, May 6). *Blockchains Networks Are Bureaucracies Par Excellence*. Medium. https://mariolaul.medium.com/blockchains-are-bureaucracies-par-excellence-db39cfda7ea9

The DAO

"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 nullify 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 Coaese'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 [1], 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 [2] 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 (developers, users) a choice 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.

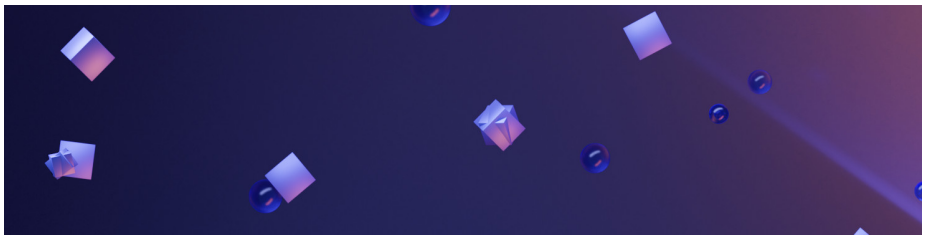
In hindsight, it seems hard to believe that people were willing to entrust so much money to a brand new initiative that was deploying its very first iteration in the wild. Even without the fatal flaws, one wonders how well such an ambitious first attempt at a DAO would have made use of the resources 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 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.

References

1. Morris, D. Z. (2016). *Blockchain-Based Venture Capital Fund Raises $100 Million And Counting | Fortune*. Retrieved 31 December 2020, from https://fortune.com/2016/05/15/leaderless-blockchain-vc-fund/
2. DuPont, Q. (2017). Experiments in algorithmic governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization. In *Bitcoin and Beyond* (pp. 157–177). Routledge. https://doi.org/10.4324/9781315211909-8

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. 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.

It is difficult to get a sense of how many Aragon 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 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.

ICO

Aragon conducted an ICO [1] 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 [1]. It seems likely that Aragon One took custody of the ICO proceeds 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".

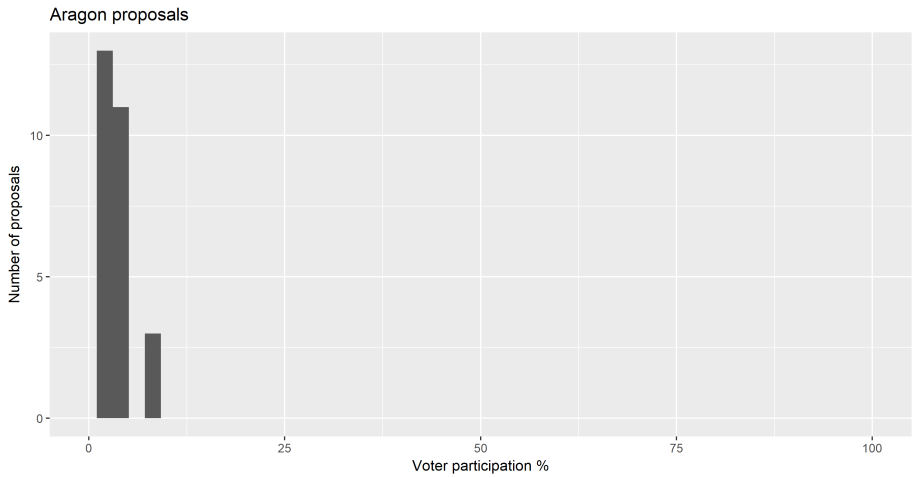
The ANT tokens themselves are utility tokens which can be used to participate in dispute resolution processes in the Aragon Network, a "digital jurisdiction" which is yet to be released.

Funding

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).

In Jan 2020 Aragon Fundraising launched, being used in the pre-activation phase for Aragon Court.

Into 2020 - Aragon Court and ANJ

Aragon Court is a dispute resolution service for DAOs, it is intended to allow for "Aragon Agreements"[2], which allow for agreements specified in human language as opposed to code, to be arbitrated. The idea is that Aragon jurors will adjudicate disputes by playing a Schelling game where they profit by choosing the same answer as other judges. People who wanted to participate as jurors could buy ANJ tokens or stake some ANT to get these, and their chance of being called on to act as judge in a particular dispute was proportional to their ANJ at stake.

Aragon Court opened with a "precedence setting" campaign [3] of mock disputes, where scenarios would be deliberated and worked through the system as if they were real, to test the system and establish basic norms for how jurors should vote. In what was a fairly major *faux pas*, the first dispute was based on a real case that had recently received attention in the crypto sphere, the actors involved were not consulted and felt uncomfortable having their case worked through the Aragon Court system. Aragon had to apologise [4]and void the mock dispute.

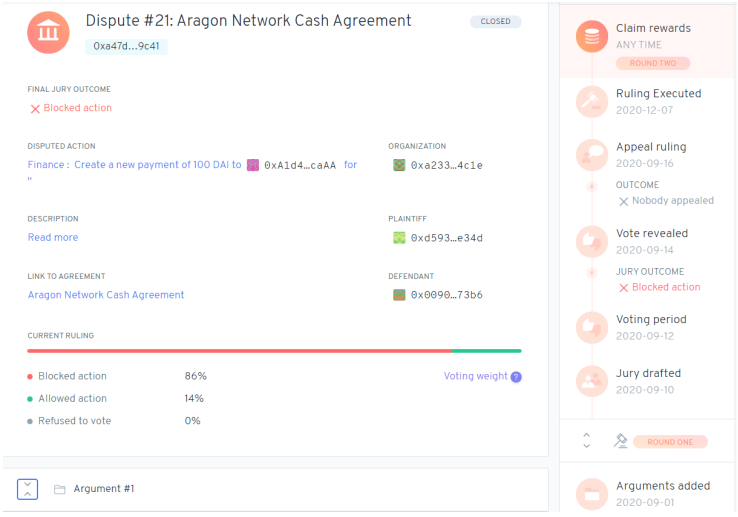


Figure 6: One of the example disputes, involving a payment for Google Analytics

So far all 22 disputes to go through Agaon Court have been of the mock variety.

In the example above (hosted on IPFS, which is an improvement on hosting these documents on Google docs or Dropbox as some other projects do) someone wanted a payment to integrate Google Analytics, but the (only) argument in the case, brought to block the payment, was that this contravened an Aragon Manifesto principle of using technology as a liberating tool. The Aragon Court jurors chose to block the payment to integrate Google Analytics in this case, with an 86% majority.

It looks like the point here is to demonstrate that Aragon isn't into tracking people, but it also paints a picture of Aragon Court as a service whereby outsiders (Aragon Jurors) will look at vague documents like a manifesto and translate them to executive decisions about the operation of your organisation.

After an aborted attempt to quickly merge ANJ into ANT, the Aragon One leadership set out a more community-led process where holders of both ANJ and ANT would get some say. The outcome of this process was fairly close to the original proposal, ANJ holders would be offered ANT at a rate of 0.015 ANT per ANJ, or a higher rate of 0.044 ANT/ANJ if they lock the ANT for a year. This will result in ~1.5-4% new issuance of ANT tokens, so in effect the ANT holders are buying out the people who participated in ANJ.

2020 changes

Here are some of the other developments which occurred with Aragon in 2020:

- Sunsetting of Aragon Chain development in favour of supporting deployment on token-agnostic Ethermint chains.
- The end of the AGP process which has allowed ANT holders to signal on proposals to spend development funds, this is being replaced with a 5 person council in phase 2 of the "Aragon Network" launch. ANT holders will be given more control of the "Aragon Network DAO" in phase 3.
- The Aragon Flock grants program was dissolved, and later the Nest grants program too, a final report on Nest gave spending figures of $1.5 Million and 271K ANT (~$888K at December 2020 price of $3.28/ANT).
- The ANT token was upgraded to ANT v2, which will be cheaper to transfer and support gasless transfers and adoption of off chain voting in Aragon v2.
- Announcement of "Aragon Govern", which is a streamlined developer-focused DAO framework.

From the DeFi space, Bancor, Aave and mstable have adopted Aragon DAOs and put significant assets under their management, although their DAOs are so far not particularly active.

Surveying the Aragon DAO scene in 2020

Since the first release of *PPCC* in Oct 2019, the DeepDAO site has launched, which tracks activity for a broad selection of DAOs active across most of the

main DAO platforms. In relation to Aragon, this allowed me to look at what the 50 DAOs tracked by DeepDAO have been doing.

The metrics for these DAOs are highly skewed, to the point where there's little point graphing them. The 3 largest DAOs have membership in the 1,000-5,000 range, but two of these have no proposals, and the other (PieDAO) has a single proposal which was voted on by just 6 members out of 3,128 total members. The two active DAOs with the most members have membership in the 100-200 range, but 38 out of 50 DAOs (76%) have 20 or fewer members. The maximum number of voters in any Aragon DAO is 24.

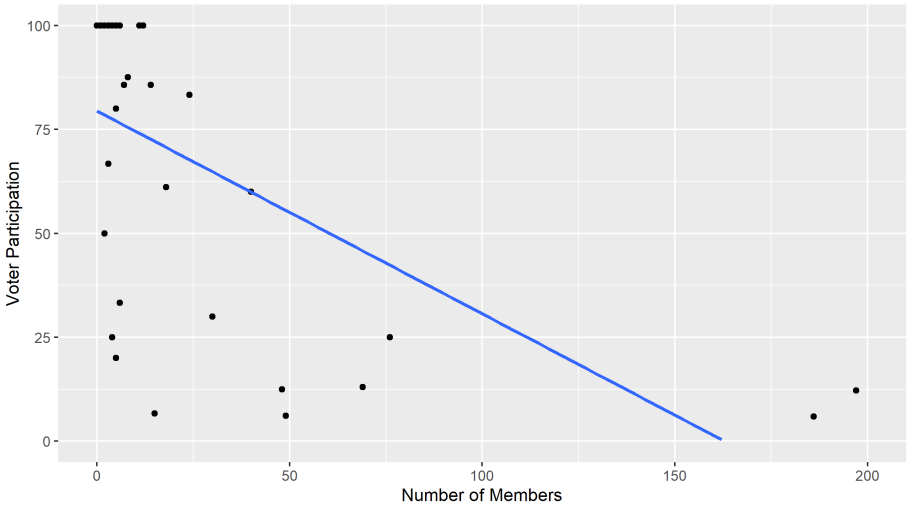


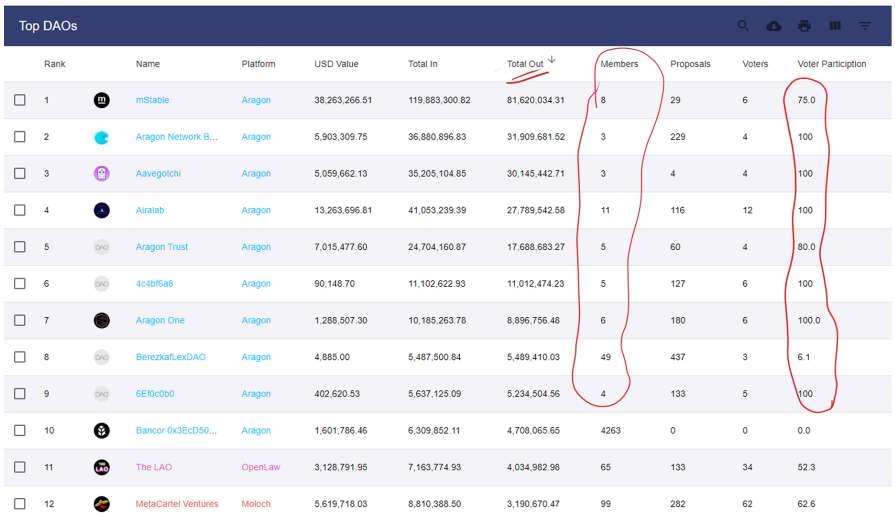
Figure 7: Scatterplot showing number of members per Aragon DAO and the voter participation (in terms of members) of that DAO - excludes 3 DAOs with >200 members. Data sourced from DeepDAO.

There is a clear relationship between the number of members of each DAO and its voter participation rate, as shown in the figure above. More members in a DAO means a smaller proportion turning out to vote. This is something you would expect to see in many systems, as the smaller the relative influence of a single voter the less it makes sense for them to spend time in exercising that influence (reading about proposals and voting).

It should be noted that the source data for above figure has values of over 100, I set these to 100 but they may indicate some underlying issue with the reliability of the measure.

Big-spending multi-sig DAOs The DAOs that have spent the most are operated by a few individuals each, with typically high participation in proposals. These DAOs are performing functions similar to multi-sig wallets, albeit

according to some breakdown of tokens as opposed to each participant having a part of the signature. Some of these DAOs are operated by the same people who are building the Aragon platform, so it is for them a case of eating their own dog-food. All of the DAO platforms engage in this kind of dog-fooding to some degree.



Top DAOs

Rank	Name	Platform	USD Value	Total In	Total Out	Members	Proposals	Voters	Voter Particiption
1	mStable	Aragon	38,263,266.51	119,883,300.82	81,620,034.31	8	29	6	75.0
2	Aragon Network B...	Aragon	5,903,309.75	36,880,896.83	31,909,681.52	3	229	4	100
3	Aavegotchi	Aragon	5,059,662.13	35,205,104.85	30,145,442.71	3	4	4	100
4	Airalab	Aragon	13,263,696.81	41,053,239.39	27,789,542.58	11	116	12	100
5	Aragon Trust	Aragon	7,015,477.60	24,704,160.87	17,688,683.27	5	60	4	80.0
6	4c4bf6a8	Aragon	90,148.70	11,102,622.93	11,012,474.23	5	127	6	100
7	Aragon One	Aragon	1,288,507.30	10,185,263.78	8,896,756.48	6	180	6	100.0
8	BerezkafLexDAO	Aragon	4,885.00	5,487,500.84	5,489,410.03	49	437	3	6.1
9	6Ef0c0b0	Aragon	402,620.53	5,637,125.09	5,234,504.56	4	133	5	100
10	Bancor 0x3EcD50...	Aragon	1,601,786.46	6,309,852.11	4,708,065.65	4263	0	0	0.0
11	The LAO	OpenLaw	3,128,791.95	7,163,774.93	4,034,982.98	65	133	34	52.3
12	MetaCartel Ventures	Moloch	5,619,718.03	8,810,388.50	3,190,670.47	99	282	62	62.6

Figure 8: The DAOs that have spent the most, have low number of members and high vote participation. Data sourced from DeepDAO.

Put your best DAO forward

On the Aragon platform 6 DAOs are highlighted, so I have also looked at those specifically.

- Lightwave has 3 token holders with an even split of tokens, it went from a max budget of 1.5 ETH to 0.2 in March 2020 and hasn't seen a proposal since.
- BrightID is a "social identity network" which aims to allow users to prove that they are unique human, its DAO has seen 101 proposals through which $780K has been spent (of $924K in). There are 11 members with an equal share (~9.1% tokens each), and they were a very agreeable bunch, with 98 or 101 proposals decided unanimously with no dissenting votes. This one operates on a minimum approval threshold where a proposal must get yes votes from >50% of tokens to be approved, and most of the proposals to fail did so without meeting this threshold, there have been 16 rejected proposals and only 1 of these had more no votes than yes. Some of these rejected proposals were simply supplanted by a subsequent proposal, this is common to many DAO communities where flawed proposals cannot be retracted and must be rejected. Most of the proposals concern

payments to workers and for organisational expenses, but there are some other types also, such as a proposal to stake tokens for the Commons Stack community.
- Livepeer is a decentralized video transcoding network and its DAO seems to have been operating from April - December 2019, it saw 30 proposals to spend LPT tokens and then all its LPT was spent and people stopped voting on proposals.
- Similar timeframe for the MyBit DAO, and the project lead leaves no room for doubt about its success with a reddit post that opens with "Hey everyone, so as I am sure most (or all) of you agree is that the project is kind of a total mess in its current stage." and explains how the remaining funds will be liquidated to held by their company.

It is clear that the rise in the cost of Ethereum transaction fees in 2020 has been hard on Aragon's DAOs, which are quite heavily "on chain" entities, and so have limited room to manoeuvre without incurring costly fees. The move to embrace a new protocol that can do more off chain, and to proffer Aragon Court as an accompaniment to something like Snapshot, are in a way pivots around the bad user experience of on chain interactions.

The following page about BlankDAO is from the initial release of *PPCC* in 2019, like many other Aragon DAOs of its vintage it seems to have gone the way of the failed experiment.

References

1. *The Aragon Token Sale: The Numbers.* (2017). https://aragon.org/blog/the-aragon-token-sale-the-numbers-12d03c8b97d3
2. *Introducing Aragon Agreements.* (2020, February 5). Aragon One Blog. https://blog.aragon.one/aragon-agreements/
3. *Precedence Campaign Primer.* (2020). Aragon One Blog. https://aragon.org/blog/precedence-campaign-primer
4. *Update on Aragon Court's first mock dispute.* (2020, February 19). Aragon One Blog. https://blog.aragon.one/update-on-aragon-courts-first-mock-dispute/

BlankDAO

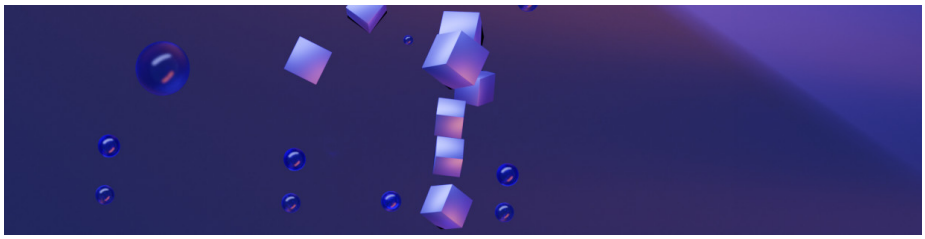
> BlankDAO is a social organization with an aim to break blockchain barriers on the road of decentralization by relying on real people instead of miners. BlankDAO is Currently an Aragon DAO

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 as "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. To this end prediction markets are used to facilitate decision-making that represents the majority's perspective, without requiring the majority to participate. This is referred to as Holographic Consensus [1].

Within a DAO, members are assigned voting tokens and the DAO can perform certain operations 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)[2] 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 stake their GEN to predict the outcomes 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 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.

On a DAOstack commons the DAO's voting members are the controlling entity,

people who would stake GEN to predict outcomes and in so doing expedite the DAO's decision-making form an interesting kind of supporting constituency. Members of the GEN predictor constituency compete with each other to more accurately predict what the voters want and in so doing earn a greater share of the rewards. Collectively, they provide a service which the DAO pays for.

It will be interesting to see how the dynamic between DAOs and their GEN predictors develops. If predictors are adequately incentivized they may put effort into detailed analysis or investigation of proposals, using this information to make a better prediction then revealing it to the DAO's stakeholders. On the other hand, without a long-term tie to the DAO's success the predictors may also try to use misinformation to push decisions in the direction they had predicted. It remains to be seen how well this kind of arrangement will work in practice, as DAOstack has only seen limited use so far.

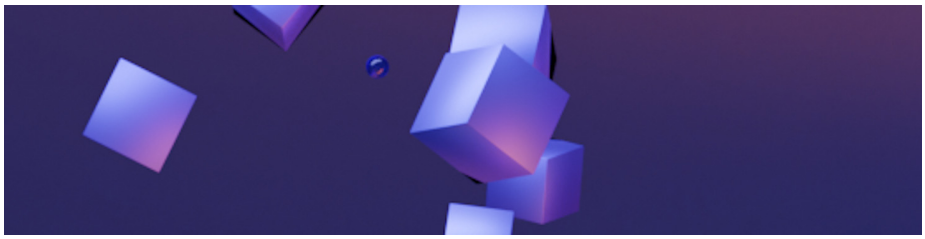
DAOstack is also an example of a project which is oriented towards addressing issues of scale that are likely to arise in the long term. The first challenge for these projects is to reach a scale of participation where their solutions can be demonstrated and tested.

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 gate-keeping 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.

References

1. Field, M. (n.d.). *Holographic Consensus—Part 2. This is the second post in the series… | by Matan Field | DAOstack | Medium*. Retrieved 30 December 2020, from https://medium.com/daostack/holographic-consensus-part-2-4fd461e8dcde
2. Zemel, J. (2018, May 16). *DAOstack Token Sale Successfully Concluded*. Medium. https://medium.com/daostack/daostack-token-sale-successfully-concluded-ec813e7adc6b

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 first writing (June 2019) it controlled 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 (100 is the standard amount to ask for), usually introducing themselves and being approved.

Looking again in Oct 2019, the proportion of reputation request proposals has dropped, there are now 283 reputation holders. Rep participation in proposals is mostly within the 2-10% range, I haven't formally collected and analyzed the data but it looks like the GEN predictions are usually (but not always) in line with the voting outcomes.

Some interesting proposals:

- Proposal to slash the reputation of the largest Rep holder by 1%, paying 1 ETH "in exchange" for the Rep lost. This is a standard practice once a member acquires more than 2% of the Rep, to avoid any one Rep holder gaining too much influence. The proposal passed.
- Proposal to fund the presence of PragueDAO at Web Summit with 6 ETH. PragueDAO is a "physical DAO" running a space in Prague, and will assign a portion of its reputation to Genesis Alpha members when its own DAO is up and running. The proposal passed, along with a number of other event funding proposals.
- Proposal to fund a research program with $3,500 DAI, the purpose of the research is to map, analyze and fix all of the issues with the current version of Genesis Protocol, and to document the process so that others can join the research effort. The research program also intends to create its own DAO-research DAO.

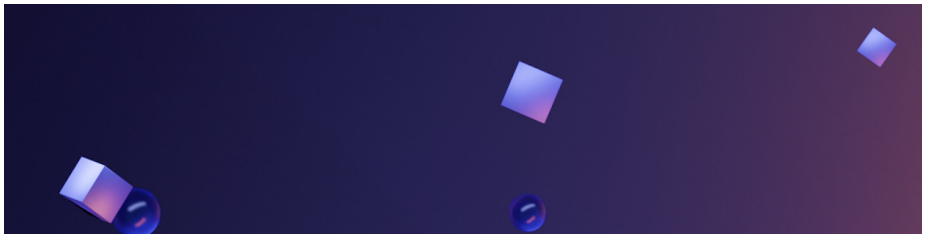
Grace Rachmany has helpfully provided an account of Genesis Alpha's decline which makes for an interesting read. By Grace's account there was a mis-match between the aims and vision of the Genesis Alpha participants and that of the DAOstack team which set up and funded Genesis. Her account of the experience makes for some interesting reading.

> The DAOfest explosion is one of the great successes and great failures of the Genesis Alpha, and it resonates with some of the previous criticism of DAO funding distribution in DASH. Basically, the problem is that people love events and meetups, and they love getting paid to put on events in their local communities. They love it so much that a tremendous amount of money ends up going towards events that don't have tangible outcomes, and even if they do, there is generally nobody accountable for maintaining the community of event organizers. The great thing about community events is that they bring in more DAO participants. The problem with community events is that they bring in more DAO participants. These new participants want to fund… more events!
>
> - The State of the DAO: Rise, Fall, and Rise by Grace Rachmany

There is also an exit letter on Google docs from two of the leaders of the Genesis DAO, these making the point about the tension between a DAO for collaboration (which the participants wanted) and one for distributing funds efficiently, with self-interested voting being for some an expected outcome and for others the thing which ruined it.

In all these materials there are also strong undertones of people joining a DAO without any strong shared idea about what it was going to be about or for. With no shared purpose it was doomed to fail.

Kyber Network



> Kyber is an **on-chain liquidity protocol** that aggregates liquidity from a wide range of reserves, powering instant and secure token exchange in any **decentralized application.**

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.

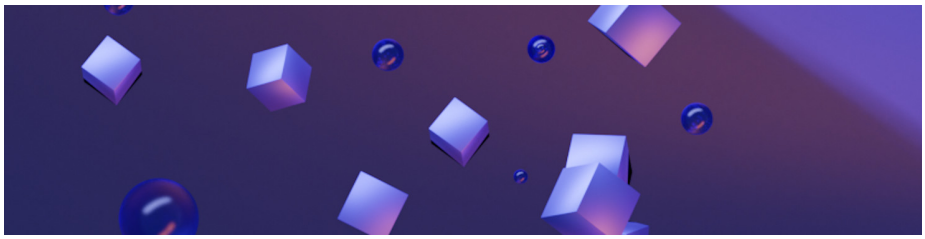
In the first experiment, an Aragon DAO was created in which KNC tokens (Kyber Network's native asset) could vote. The first proposal asked whether

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.

The Kyber DAO Exp#2 using DAOstack launched in Jun 2019, awarding Rep to KNC holders and people who had traded on Kyber in the previous 3 months, according to a scale determined by their holdings/activity. Participation in the DAO proposal votes was low, with a maximum participation of less than 1% of Rep. Most of the proposals failed because there was insufficient voting turnout and they failed to achieve majority support. Writing in Oct 2019, the DAO still has $500 of KNC to spend, but proposals and votes have become scarce.

Kyber's efforts illustrate 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 another 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.

dxDAO



dxDAO is a DAO that has been created to govern the DutchX protocol.

> The **DutchX** is a fully decentralized trading protocol that allows **anyone** to add any trading token pair.

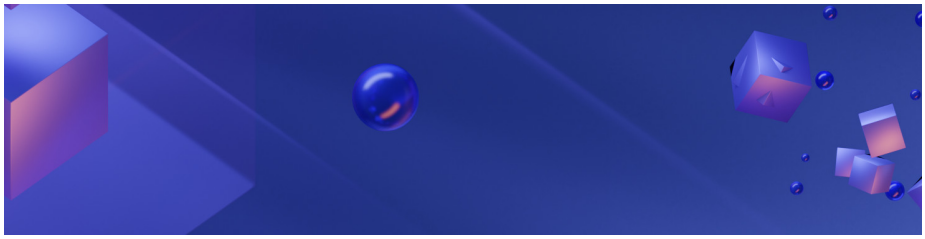
The DutchX was produced by Gnosis (Ethereum futarchy organization and token), who then wanted to hand the ongoing governance off to a DAO. To this end, they held a staking event (or "lock drop") where interested parties could participate to gain Rep in the dxDAO. 50% of the Rep went to people who registered MGN tokens (earned by trading on DutchX), 30% to people who time-locked whitelisted tokens, 8% to people who time-locked ETH, and 10% to people who bid GEN tokens.

As of Oct 2019 dxDAO lists 400 members. Rep is quite concentrated, the top Rep holder has 10% and the top 10 holders control ~58% of the Rep. The history page is throwing an error right now so it's not possible to look at how previous

votes have gone and what they have been about. Open proposals concern de-whitelisting ANT, LOOM and REQ tokens as MGN generating tokens, they are all set to pass with unanimous approval from 8-16% of the dxDAO Rep tokens.

This is in line with dxDAO's stated purpose, which is to make changes to the smart contracts of which the DutchX is composed. I'm not sure if there is a mechanism to redistribute dxDAO Rep over time, in particular to allocate some to new users of DutchX. The idea to put governance in the hands of the platform's stakeholders is a good one, but allocating all of the voting rights at such an early stake would likely be sub-optimal in the long run, with early users holding all of the power to decide how the platform develops.

Moloch DAO



Moloch is a set of Ethereum smart contracts which form a DAO, people submit tribute with their requests to join and the tribute of members forms the DAO's treasury. Members vote with their shares on whether to spend some tribute to fund proposals. The smart contracts for Moloch have been cloned many times by different groups to create their own Moloch style DAOs, one of these is considered in the following section.

The original Moloch DAO launched in February 2019[1] for funding development of the Ethereum ecosystem. Members of 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 had been completed, and a further 10 were 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.

In 2020 Moloch DAO got up to speed and started spending, according to DeepDAO data it has now (Dec 2020) spent $3.6M. It is up to 76 members, 130 proposals have been voted on (includes 66 proposals to add new members), and it has a remaining balance of 3,000 WETH.

One useful way to look at Moloch participation is in terms of number of users, because every address represents an individual member which went through its own application process (although Ethereum Foundation has 10 numbered "seats").

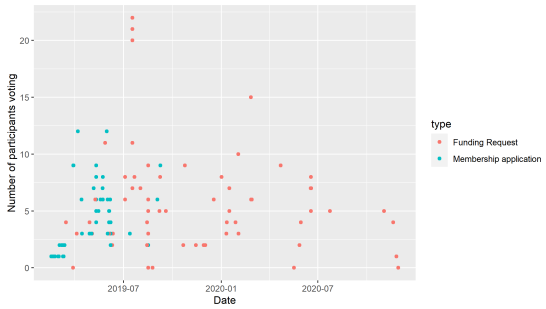


Figure 9: Moloch proposals and the number of members who voted on each

The mean number of members who vote on a proposal is 5, in 2019 this covers a period where there were many proposals to onboard new members which had just 1 vote each, and also a period of greater voting activity. In 2020 the mean for the year is 5.4. This is not very high turnout, a few members are making decisions on behalf of the DAO. Moloch is however designed to accommodate this, with the option for members to ragequit and reclaim their share of the pot if they don't like a proposal which is to be funded.

The graph indicates a slowdown of proposal activity over the course of 2020 thus far.

The way it is being run, Moloch DAO looks like it's being used as a vehicle for the large members (who provided the most tribute but don't vote) to soft delegate spending decisions to members with lesser stake but who are (presumably)

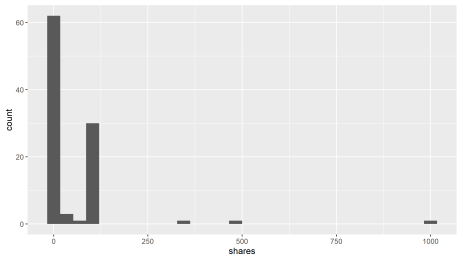


Figure 10: Moloch members histogram

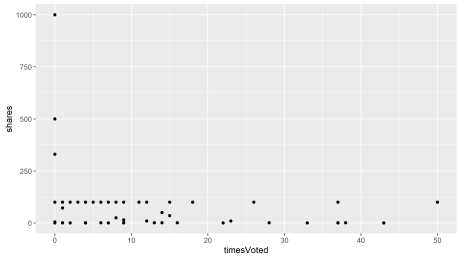


Figure 11: Moloch members shares and number of votes

putting in the time to consider funding request proposals in detail before voting on them. Notably the 3 largest shareholders have never voted.

Among the voting members there is a divide between those with ~100 shares and those with ~1 share, the latter group having little effective say.

Moloch Clones

As soon as Moloch was released we began to see new Moloch type DAOs popping up [2] for such diverse purposes as organizing a Year of DAOs event and Whisky tasting party (OrichiDAO), and supporting the Presidential campaign of Andrew Yang (YangDAO).

These Moloch clones signal competition for DAO platforms like Aragon and DAOstack. A Moloch type DAO is much simpler, with many fewer lines of code, than a DAO on one of the platforms. Complexity makes software harder to secure, and so simpler DAOs may have an advantage when it comes to larger sums. There are also no fees involved in cloning and editing a set of smart contracts that are already publicly available.

In 2020 the DAOHaus site launched, which showcases the Moloch concept and DAOs, and provides some learning material.

References

1. Moloch. (2020, January 1). *Moloch—2019 Year in Review*. Medium. https://medium.com/@molochdao/moloch-2019-year-in-review-eb6f53dc035

2. Waugh, J. (2019, October 16). *Relearning to DAO craft*. Medium. https://medium.com/axialabs/relearning-to-dao-craft-b815b3e3f8ef

MetaCartel (Ventures)

MetaCartel (Ventures)

MetaCartel was one of the largest Moloch clone DAOs and it served to distribute funding to an "ecosystem of DAPP builders" in the form of grants. According to DeepDAO, MetaCartel dispensed $620K in funding (not counting $355K which was migrated to v2), seeing a total of 137 proposals approved of the 146 submitted.

MetaCartel migrated to a Moloch v2 DAO, these allow funds to be issued in a less convoluted way that does not require the recipient tom ragequit shares to receive spendable funds. The v2 DAO is still going, it has $60K left from the $443K it has received to date.

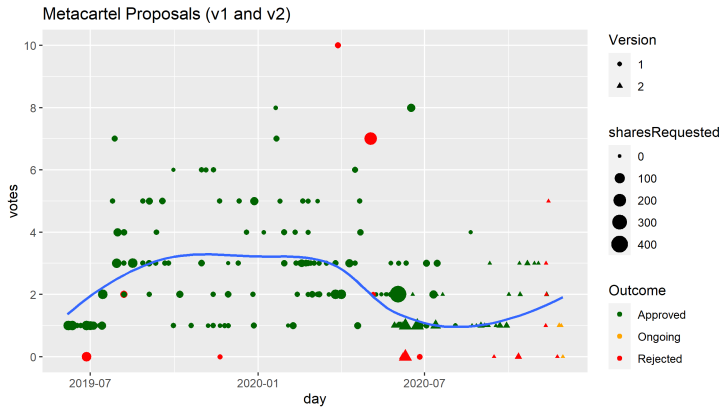


Figure 12: MetaCartel DAO Proposals: Number of voters (Y axis), version (1 or 2) and shares requested (size)

From the graph you can see that the number of accounts voting on each proposal is fairly small, for v2 this has dropped down to 0-3 voters per proposal. Most of the proposals that are voted on pass, with many rejections happening without anyone voting on the proposal.

MetaCartel also has a bigger sister DAO now, **MetaCartel Ventures**, which is a pivot to DAO as instrument of a conventional for-profit enterprise - or in other words, the DAO funders are now able to take equity positions and other considerations in exchange for funding. This DAO has a much larger balance, with $6.1M AUM (Dec 12 2020), and having already spent $3.8M. There is a private forum where details of deals are shared with DAO members, but the votes are publicly visible, and I can see that recently approved investments include Rarible and BrightID.

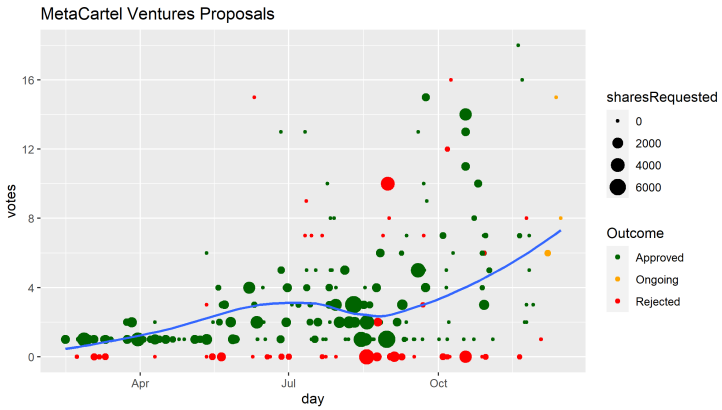


Figure 13: MetaCartel Ventures Proposals: Number of voters (Y axis), outcome (colour) and shares requested (size)

The Ventures DAO is sustaining a higher number of unique participants in its votes, although the maximum number to participate in a proposal is only around 18 out of the ~100 total members. In addition to proposals on investments, most of the proposals are for things like "DAO Member of the Month" and share awards, but also "Tax accounting services".

The LAO

The LAO

"**The LAO**" is another Moloch type DAO with the "rage quit" concept, which has joined forced with Moloch and MetaCartel. The LAO is designed to work with and serve a legal entity in Delaware, so instead of aiming to be its own independent entity it is being used to serve some functions within a more conventional organization.

The LAO is more secretive with the names for its proposals, and so less can be inferred about what the members are voting on.

The graph shows that The LAO is using the Moloch contracts differently, I assume proposals with large share requests are new members and these have

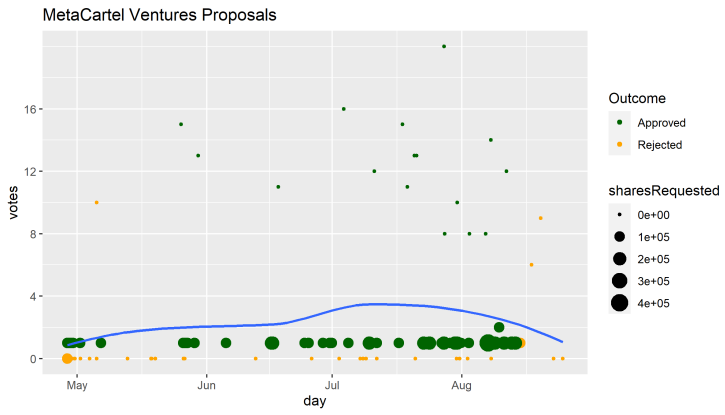
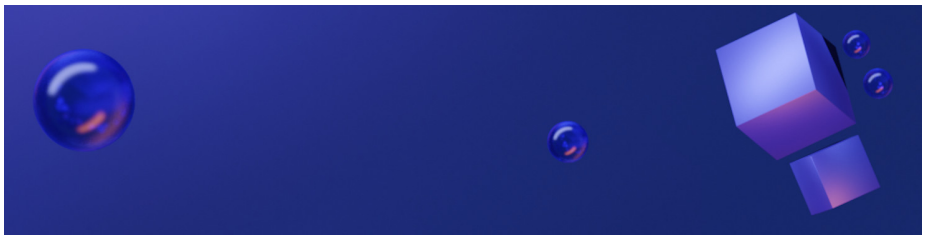


Figure 14: The LAO Proposals: Number of voters (Y axis), outcome (colour) and shares requested (size)

been pre-approved, hence only being voted on by one member to approve them. The votes with 8-20 participants are likely about substantive matters like investments. The LAO has a total of 65 members, $3.7 AUM (Dec 20 2020), and has already spent $4.5M.

For these venture-oriented "DAO"s the DAO is really just a convenient structure to use for handling funds, but secondary to the legal entity in terms of its capacity to make decisions about those funds. Whether these entities are successful depends on whether their members make good investment decisions, but the idea that it is a DAO that's in charge and that people can engage in this kind of activity through a DAO is far-fetched. In the case of any major issue with these DAOs' operation, things will proceed according to whatever is written in the legal entity's specifications and contracts.

Maker DAO



Crypto Governance Research excerpts

This section is composed of excerpts from an overview[1] written by Seth Benton in mid-2019, 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 determining the risk parameters that are used to manage the portfolio of assets backing DAI (at time of writing just ETH, but soon others with the introduction of multi-collateral DAI).[2]

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 cadence. 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.

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 modelled 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 [3] 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.

The Maker DAO Commons

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 Aug 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.

In Nov 2019 Maker launched Multi-Collateral Dai (MCD) [4], which went on to become just DAI, (and single collateral DAI became SAI).

In March 2020 Maker experienced its most challenging episode yet, on "Black Thursday"[5] when the price of ETH crashed (along with other assets) the ETH backing many DAI positions was liquidated, and in some cases (36%) the liquidation auction malfunctioned due to on chain congestion and the ETH was given away for nothing. It was estimated that $8.3M was lost in these liquidations. Someone realized that they were one of the only people who had figured out how to get bids in by increasing the gas fee, and they bid pennies on liquidation sales, securing lots of up to 50 ETH for nothing. To its credit though the system did not collapse entirely, and the Maker team will have learned from this experience how to avoid the same thing happening in future.

Black Thursday has left a lingering hangover in the form of a class action lawsuit from investors seeking $28M [6] for losses on the basis that the Maker Foundation knowingly misrepresented the risks involved in using the platform. The MKR holders have voted no on a proposal to compensate Black Thursday victims, with 65% of tokens voting for zero compensation[7]. This dispute is an interesting one to watch as it sets expectations for how the MKR and DAI stakeholders will interact when the platform has a technical issue which impacts users financially.

In late October 2020 flash loans became another thing for Maker's governors to worry about, as BProtocol flash-borrowed 13,000 MKR to vote for their own proposal.[8] In this case they were already winning and just speeded the process along, so no harm done, but it still prompted a discussion of how to disincentivize MKR holders from leaving their MKR in a liquidity pool where it can be used to attack the project, until such times as this attack vector can be addressed.

References

1. Benton, S. (2019, May 20). *MakerDAO*. Block Commons. https://www.blockcommons.red/crypto-governance-research/overviews/maker/

2. Hoffman, D. (2018). *The Role of Ether in Multi-Collateral DAI | by David*

Hoffman | POV Crypto | Medium. https://medium.com/pov-crypto/the-role-of-ether-in-multi-collateral-dai-cfc8b43ab50c

3. Cuen, L. (2019, March 5). *MakerDAO Opens Token Holder Vote on Fee Hike for Ethereum Stablecoin*. CoinDesk. https://www.coindesk.com/makerdao-dai-fee-hike-vote

4. *Currency Re-imagined for the World: Multi-Collateral Dai Is Live!* (2019, November 18). Maker Blog. https://blog.makerdao.com/multi-collateral-dai-is-live/

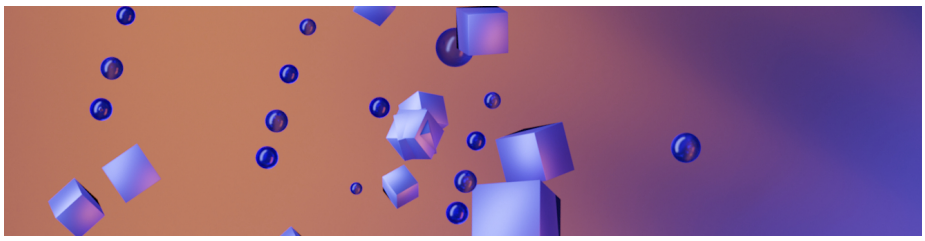
5. whiterabbit. (2020, Mar 14). *Black Thursday for MakerDAO: $8.32 million was liquidated for 0 DAI*. Medium. https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6

6. *$28M MakerDAO 'Black Thursday' Lawsuit Moves to Arbitration*. (2020, September 29). CoinDesk. https://www.coindesk.com/28m-makerdao-class-action-lawsuit-arbitration

7. Makerdao Vote to Not Compensate Black Thursday Victims Receives Harsh Criticism. (2020, September 24). *Bitcoin News*. https://news.bitcoin.com/makerdao-vote-to-not-compensate-black-thursday-victims-receives-harsh-criticism/

8. *'Flash Loans' Now Being Used to Manipulate Protocol Votes*. (2020, October 29). CoinDesk. https://www.coindesk.com/flash-loans-manipulate-defi-protocol-elections

Decentralized Finance



DeFi has been driving a lot of the news, social media and market activity in 2020, with a number of Ethereum-based decentralized exchange and lending protocols gaining significant traction. One of the top memes here was **yield farming**, finding ways to deploy capital assets in a way which would generate attractive yields - often involving stringing a number of different protocol transactions together (**composability**).

The Defi Pulse site is good for getting a quick sense of what's hot in the DeFi space, with "total value locked", the capital deployed with a platform, taken as a key measure of success. DeFi markets are driven by people "locking" an

asset that has value in a way that allows them to derive a yield from it. The key assets being locked are ETH (as Maker DAI stablecoin), Bitcoin (as WBTC, renBTC) and other Ethereum-based tokens. The tokens issued on the basis of this collateral are the fuel which powers the DeFi ecosystem.

DeFi Foundations

The process of locking a crypto-asset to obtain something is not risk-free, and each of these services presents a different kind of risk. These warrant a mention, because the stablecoins and wrapped assets are also foundational for the rest of DeFi. Most of the methods involve relying on some centralized custodian to perform minting/burning functions and track the balances, like Tether (backed by a company), WBTC (backed by a consortium of companies), renBTC (backed by a multi-sig). In these cases the assets are as secure or robust as the backing entity, and most of them have ways in which transactions and balances can be selectively censored/nullified.

MakerDAO and the DAI asset take a different approach which aims to be more decentralized by removing the centralized custody of assets from the equation. Instead, collateral (initially ETH, now any of a basket of Ethereum-based tokens) is locked up in an on chain transaction, allowing a certain amount of DAI to be minted. The rate at which the DAI is backed, and associated fees, can be controlled by Maker token holders through executive votes to approve changes to the protocol. Rate changes offer certain levers that can be pulled to try and encourage the DAI price to behave as desired (stability at 1 DAI = 1 USD), but this cannot be forced by the system. There have also been issues where the system behaved in unexpected and problematic ways while under strain, such as the "Black Thursday"[1] event in March 2020 when $8.3 million of collateralized ETH was "sold" for nothing in auctions that didn't have any bids, leading to losses for some users which are still being litigated [2] after MKR holders voted [3] to not compensate these users.

Maker's DAI has a very different risk profile to the centralized stable-assets, it lacks some of the failure modes of older assets like Tether, but as with any system that derives strength from decentralization, it's important to ask *how decentralized* Maker's governance is. Key factors here are relatively concentrated MKR balances, such that relatively few people are needed to form a majority of voting power, and votes typically have around 40 participants total. There are also major roles for the Maker Foundation and a risk team, who prepare the proposals that MKR holders will approve. Originally Maker Foundation members had an executive shutdown key which could be used to halt the system and liquidate collateral, should something go catastrophically wrong. This has been disabled, and triggering the emergency shutdown now requires 50,000 MKR to be deposited to a contract address.

Although the absolute number of participants is not large, the Maker DAO members are making extensive use of the polling and executive votes - 355

polls have been completed and many executive votes (mostly adjusting fees) in the ~15 months since it was adopted in August 2019. The executive votes run continuously, and are constructed by the risk team, which itself has polling proposals to establish support for its actions. This is at least an impressively comprehensive record of the actions taken in the governance of DAI.

MakerDAO is taking on challenges which are non-trivial to address, the system has exhibited some undesired behavior but it is probably the most or only decentralized stablecoin and has been widely adopted within the Ethereum ecosystem. This is a great success for Maker, and establishes it as important within the ecosystem, which should give it some clout in Ethereum's governance.

Yield Farming Mania

The point at which I personally realized I could no longer ignore DeFi was when YAM appeared [4] on the scene and became wildly popular (and profitable) for a brief few days, before turning into the subject of a successful last-ditch community mobilization effort, which then failed because of a second unforeseen critical issue. I found it funny, and also intriguing, that something which was billed as a "governance token" could acquire so much (notional) value so quickly, despite being so bad at what it was aiming to do - the system was set up so that all the funding would become un-spendable within days, the dev fund turning into a black hole that swallowed the whole project.[5] All of this happened within the space of about 3 days. Yam was pitched as a monetary experiment, it mashed up aspects of some popular DeFi protocols to produce an "elastic supply cryptocurrency, which expands and contracts supply in response to market conditions, initially targeting 1 USD per YAM", and additionally buying yCRV tokens with the supply expansion and placing these in the Yam treasury.

YAM was a monetary experiment, composed of several other monetary experiments wrapped together in a package that didn't quite work.

But the YAMs were just an appetiser for a more substantial meal with several courses, featuring food tokens from up and down the pyramid and most notably SUSHI. I have written an overview of Sushiswap and Uniswap, focusing on their governance and recounting a version of the story so far. Some highlights for this post are:

- Automated Market Makers are a novel way of creating markets that don't rely on the conventional order books but instead have participants add and withdraw tokens from pools to make trades, with smart contract logic determining prices.
- Bancor pioneered AMM pools, but Uniswap popularised the idea with a method that didn't involve buying special tokens to participate.
- SushiSwap copied Uniswap's smart contracts, dropped the idea that a fee would be added to compensate VC investors and added in a SUSHI token instead, which would be distributed to all of the liquidity providers (effectively the people who run the AMM service). This also incorporated

a "vampire attack", where SUSHI tokens were being offered specifically to Uniswap liquidity providers at an attractive rate, so as to lure them and their liquidity into the competing SushiSwap pools.

- The story had drama, when Chef Nomi made an abrupt transition from being the hero who founded SushiSwap to liquidating the entire SushiSwap dev fund and pocketing the ETH. The Chef would later return the ETH, and it would be converted back to SUSHI, but his reputation in the community had been irreparably damaged.
- Uniswap subsequently added a UNI governance token which works in a very similar way to SUSHI, and made a retroactive initial distribution of these tokens to people who had used the Uniswap decentralized exchange. The UNI token started trading at around $2-4, and 150 million tokens were distributed initially, so this amounted to an almost instantaneous creation of about ~$500 million in value. In UNI's case the token was capturing value that had been developed in the protocol with a claim on its future governance and some fee revenue - but SUSHI performed similar alchemy with largely borrowed tools.
- Uniswap won most of its liquidity providers back from SushiSwap when UNI launched, but as initial bonus incentives expired and SushiSwap responded with more of its own bonus schemes the liquidity has started to tilt back in SushiSwap's direction. In either case it seems there will be ongoing competition between these protocols, and one of the only differentiators will be their governance.
- The overview covers the governance of the respective projects in some depth. While similar in outline the use of the proposal systems is very different in the production environment, due largely to the different thresholds for creating and approving proposals. Just before the end of 2020, Uniswap had its first governance proposal approved, to fund a grants program with up to $750K quarterly. The program will be administered by a committee of 6 members with 1 lead (all named in the proposal).

Yearning for Decentralized Finance

Yearn Finance, with governance token YFI, is a set of smart contracts created by Andre Cronje which aims to provide access to yield-farming and other profitable opportunities to people who put their assets in vaults that manage allocated funds according to a specified strategy. Brady Dale of Coindesk has written extensively about what Yearn is about[6] and the manner in which it has expanded through a series of mergers to position itself as the "Amazon of DeFi". [7]

Yearn, and a similarly purposed Harvest finance, serve as an easy on-ramp to engaging in DeFi yield maximizing, their aim is to do this for the user within defined parameters. This allows more capital to be engaged in these markets and pools than would otherwise be the case.

In terms of Yearn's governance, it is worth noting that it had a "fair launch", with no premine of the YFI token. Early in the project's history it was decided

to issue 30K YFI tokens to people who were providing liquidity over a one week period. This is how all of the YFI tokens were issued, and the YFI holders have subsequently voted to reject proposals to issue more YFI.

Governance takes place primarily in the forum and snapshot is used for voting. Snapshot signal voting is popular among Ethereum projects which use voting in their governance, as it allows for votes to be cast without incurring gas costs. Snapshot was developed by Balancer labs, another DeFi project.

Control of the YFI minting contract was put in the hands of a 6 of 9 multi-sig Gnosis Safe, and Andre Cronje removed himself as one of the controllers. This was seemingly done because Andre had the exclusive rights to mint YFI before and this became a bigger key man risk with the rise in value of YFI. The forum post refers to another forum post with details of the on chain voting system for approving changes to smart contracts, but at the time this appeared to be largely aspirational and still at the "Andre does it manually" stage.

As Yearn has embraced a strategy of partnership and mergers in recent months, the prize vegetables from the year's bumper food token crop which didn't rot in the heat of DeFi summer are now being combined, and the table is set for a soup-er 2021 (puns intended, sorry).

It's on fire!

When it comes to the DeFi space as a whole, hacks and failures (sometimes spectacular) have been a regular occurrence in 2020.

There have been a great variety of these, including some novel types previously unseen, such as the **flash-loan** attack pioneered [8] on the bZx Ethereum dapp. A flash loan is a novel type of credit offering where large sums can be borrowed with no collateral but must be paid back within the same block. In other words, a flash loan only works as part of a chain of transactions, all executed within the same block, starting with the loan being taken out and ending with its repayment in full. If anything goes wrong with the series of transactions and the amount is not repaid, the flash loan simply fails to make it into the blockchain, and leaves no trace.

The atomic resolution virtually eliminates risk to the lender's capital, and this means they can lend to anyone with good assurance of being repaid, plus one assumes a fee to make it worth the lender's trouble. This has a levelling effect, because previously the amount of money one could make from exploiting bugs in DeFi smart contracts was limited by the amount of capital one could deploy.

This paper by Qin, Zhou, Livshits & Gervais [9] dissects the first two flash loan attacks in detail, and offers notes on how to increase the profitability of the technique. The technique for these hacks involved using some of the loan to manipulate a price oracle while using the rest to make transactions which would profit from the manipulation. The first two flash loan attacks netted less than $1 million, whereas as the year went by the sums being gained by people using

flash loans to exploit smart contracts increased considerably. Someone flash harvested $24M from Harvest Finance in October, flash spoils of $7M, $6M, $2M in November - and those are just the recent examples.

The fault here lies primarily with the DeFi protocols which have such weaknesses, the flash loans just open up the possibility of making money from these exploits to people who don't have their own capital to deploy. This seems to be the emerging consensus.[10]

According to ciphertrace's blog post[11] DeFi accounts for around 48% of the number of crypto hacks/thefts, and around 30% of the volume of lost funds - up from virtually negligible last year.

As an outside observer, the impression that the more vocal "DeFi degens" make on twitter is that they're in solid profit and can take these losses on the chin.

Seeing the Ethereum community pile hundreds of millions of USD worth of crypto assets into novel smart contracts is an interesting spectacle. The speed of development and deployment, and the gusto with which pools are filled with assets, echo the "move fast and break things" style of development - for the community it could be extended as "move fast and tolerate risk". This feels to me like one of the characteristics of blockchains which align with personality traits, such that people will be drawn to different projects based on how comfortable they are with risk and complexity. If we consider the range of "potentially hazardous unknown events" that could befall users of Bitcoin as compared to dForce, for example, it's a totally different ball game.

Dark Forests in Ethereum Land

Flash loan attacks are an example of a profitable transaction which could be executed by anyone, and so they are in theory susceptible to poaching or front-running by miners and other nodes which will relay the transaction to miners. This kind of front-running has been observed previously by Daian et al. (2019)[12] and given the label "miner extractable value" (MEV).

In 2020 I enjoyed two articles about dealing with this "dark forest" (referencing the "Three Body Problem" science fiction series) from the perspective of developers who were aiming to "rescue" some vulnerable funds. In the first one [13], by Dan Robinson and Georgios Konstantopoulos, the protagonists try to sneak a burn transaction past the mempool bots which they suspect are lurking, but it gets picked off in a few seconds and the miner pocketed $12,000. The second [14]story on this subject, from samczsun, had higher stakes, benefitted from lessons learned in the earlier attempt, called in expert help, and was ultimately successful in the rescue of $9.6 million which had been sitting in a vulnerable smart contract by enlisting the help of a miner who could mine the transaction directly. I thought both of these were well written and interesting accounts of the true nature of the Ethereum mempool and one of the ways in which miners exert control over the network.

Doxxed hackers and donations

There have been a few DeFi-related incidents in 2020 that ended with the attackers giving some or all of the ill-gotten tokens back. Perhaps most notably, whoever hacked the dForce smart contracts for $25 million of deposited crypto went on to return almost all of it, $23.8 million (they lost money on some trades before returning everything). In this case it seems clear that the hacker's identity was exposed and they opted to return funds to avoid possible repercussions.

Doxxing, or having one's identity exposed, is also a possible explanation for Chef Nomi's return of the Sushi development funds.

One of the larger hacks of the year had a more conventional and centralised target, the Kucoin exchange, which was hit for $275 million. A report [15] by Chainalysis gives details of how the hacked funds were processed and make a point about the growing use of DeFi decentralized exchanges to swap the tokens into something less obviously stolen, making it more difficult for exchanges to block transactions which use these stolen funds. The trace is easy for an outfit like Chainalysis to follow however, and they seem to have been involved in providing information which led to the freezing or burning [16] of a significant proportion (~65%) of the stolen tokens.

This relates back to the point above about the foundations of DeFi (and dapp tokens generally). The following projects were able to move swiftly to censor the hacker's funds: Orion Protocol, Covesting, Kardiachain, Velo, VIDT, Silent-Notary, Ocean Protocol and Tether.

I have been spending some time analysing the Decred blockchain in 2020, and I have seen for myself the unreasonable effectiveness of address clustering[17]. UTXO chains like Bitcoin and Decred afford more options for tactical use of addresses, as a wallet can generate many addresses and these are not linked unless used at the same time (as common inputs to a transaction). Without careful UTXO selection, addresses are likely to be combined in such ways as to allow someone who knows about one of a user's transactions to know about many more of their transactions and balances.

Ethereum is account-based, and this presents further challenges, it is perhaps a more difficult environment to protect one's privacy in. It is noteworthy however when even people with presumably a high degree of proficiency with this technology (enough to exploit a bug in a smart contract) have to give their loot back because they revealed their identity by mistake.

Cryptocurrency is a double-edged sword when it comes to illicit uses. Censorship resistance (where this is actually provided by the cryptocurrency) means nobody can stop its use for a criminal purpose, but the price is sharing details of one's transactions with thousands of nodes around the world to be included in a permanent public record.

This is not just a problem for criminals, but anyone who could become a target

if details of their cryptocurrency transactions or holdings became known to nefarious actors. In my view this is a significant obstacle to a future where self-custodied cryptocurrency is common among the general population. Privacy is a major component of practical security when it comes to cryptocurrency.

There have also been some crypto donations by hackers who weren't necessarily exposed but maybe just felt like indulging in some Robin Hood type behaviour.

One such instance concerned DeFi legend Andre Cronje, who was testing a new protocol/token (EMN) in prod and tweeting about it when overnight people deposited $15 million worth of assets into the new unaudited contracts and it all got taken by someone who spotted a flaw in the contracts. Half of the funds were returned to the contract which Cronje controls, and he tweeted that they would be distributed to EMN holders based on a snapshot of addresses.

Maybe this is catching on as part of a broader trend, because it seems like now a group of ransomware hackers have started making charitable donations.[18]

References

1. whiterabbit. (2020, October 2). *Black Thursday for MakerDAO: $8.32 million was liquidated for 0 DAI.* Medium. https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6

2. *$28M MakerDAO 'Black Thursday' Lawsuit Moves to Arbitration.* (2020, September 29). CoinDesk. https://www.coindesk.com/28m-makerdao-class-action-lawsuit-arbitration

3. Makerdao Vote to Not Compensate Black Thursday Victims Receives Harsh Criticism. (2020, September 24). *Bitcoin News.* https://news.bitcoin.com/makerdao-vote-to-not-compensate-black-thursday-victims-receives-harsh-criticism/

4. Yam Finance. (2020, August 17). *YAM: An Experiment in Fair Farming, Governance, and Elasticity.* Medium. https://medium.com/yam-finance/yam-finance-d0ad577250c7

5. *DeFi strikes again: YAM protocol bug leads to $750,000 loss.* (2020, August 14). CoinGeek. https://coingeek.com/defi-strikes-again-yam-protocol-bug-leads-to-750000-loss/

6. *What is Yearn Finance? The DeFi Gateway Everyone Is Talking About.* (2020, September 8). CoinDesk. https://www.coindesk.com/what-is-yearn-finance-yfi-defi-ethereum

7. *Mergers Position Yearn Finance as the Amazon of DeFi.* (2020, December 14). CoinDesk. https://www.coindesk.com/mergers-position-yearn-finance-as-the-amazon-of-defi

8. Qureshi, H. (2020, February 27). *The DeFi 'Flash Loan' Attack That Changed Everything*. CoinDesk. https://www.coindesk.com/the-defi-flash-loan-attack-that-changed-everything

9. Qin, K., Zhou, L., Livshits, B., & Gervais, A. (2020). Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. *ArXiv:2003.03810 [Cs]*. http://arxiv.org/abs/2003.03810

10. *DeFi Exploits Can't Be Pinned on Flash Loans, Industry Leaders Say*. (2020, November 18). CoinDesk. https://www.coindesk.com/defi-exploits-flash-loans-industry-leaders

11. Jevans, D. (2020). *Half of 2020 Crypto Hacks are from DeFi Protocols and Exchanges—CipherTrace*. https://ciphertrace.com/half-of-2020-crypto-hacks-are-from-defi-protocols-and-exchanges/

12. Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., & Juels, A. (2019). Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. *ArXiv:1904.05234 [Cs]*. http://arxiv.org/abs/1904.05234

13. Robinson, D. (2020, September 21). *Ethereum Is a Dark Forest*. Medium. https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff

14. Samczsun. (2020, September 24). *Escaping the Dark Forest*. Samczsun. https://samczsun.com/escaping-the-dark-forest/

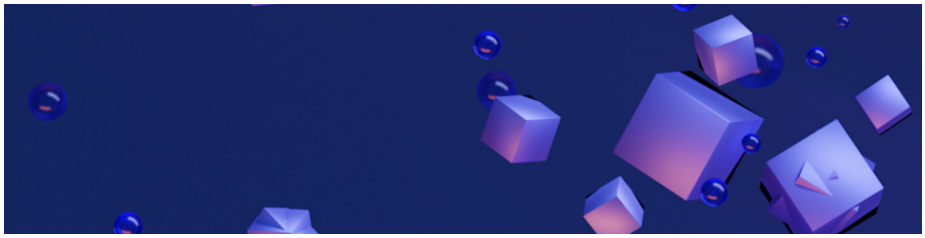
15. *Chainalysis Blog | The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds*. (2020). https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap

16. Stevens, D. / R. (2020, September 27). *$130 Million of KuCoin Hacker's Haul To Be Frozen by Crypto Projects*. Decrypt. https://decrypt.co/43066/130-million-of-kucoin-hackers-haul-to-be-frozen-by-crypto-projects

17. Harrigan, M., & Fretter, C. (2016). The Unreasonable Effectiveness of Address Clustering. *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, 368–373. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0071

18. Mysterious 'Robin Hood' hackers donating stolen money. (2020, October 19). *BBC News*. https://www.bbc.com/news/technology-54591761

Social Tokens, Crypto-gated Communities



One of the emerging trends of 2020 has been "Social Tokens", where people issue their own tokens for various purposes, some of which seem to border on securitizing the self. Colin Harper has written about how personal tokens raise red flags [1], and those are all valid concerns, but as he notes they do not seem to be preventing many people from launching this kind of token.

Some examples:

- Frenchman Alex Masmej, 23 years old, recently raised $20,000 on Ethereum by tokenizing himself. Now he wants his investors to vote on his life choices - Coindesk [2]
- FC Barcelona's Token Sale Hit $1.3M Cap in Under 2 Hours - Coindesk [3]
- Lil Pump Is Doing a Social Token Called PumpCoin - Coindesk [4]
- Rapper Lil Yachty Sells Out Social Token in 21 Minutes - Coindesk [5]

When established entities with large followings like Barcelona FC start experimenting with using tokens to promote engagement, it starts to seem likely that this kind of token will be the first contact many people have with blockchain technology.

There's an app (tryroll) which allows anyone to easily mint their own tokens and suggests they start offering services in exchange for these tokens.

There's a platform (fyooz) which invites readers to "Become a token", complete with big flashy image promoting the concept to "Monetize Your Fame", there may be some brainwashing attempt going on there so be careful not to get sucked in. At fyooz, token generation is a more bespoke affair and is more for people with fame to monetize, like Lil Yachty.

A new and interesting trend I noticed in relation to "Social tokens" is the private Telegram channel which requires a balance in some token to access. Private groups and "paid groups" are not new of course, and are notoriously the domain of con artists, but the token-secured Telegram chats are an interesting development that seems to be working for some communities. "Access" is one thing

that anyone can sell, and there are tools now which can tie that access to a token, thus providing a practical feature of that token which can be delivered in an observable and ongoing way. In the process this kind of barrier can make community management much easier as it makes the group less accessible to casual trolls and attaches a real cost to an account.

These private channels seem to be central to the appeal of a number of social tokens in this optimistic overview [6], along with promises about shares and airdrops which are probably not binding in any meaningful way.

Restricted access to a discussion channel is also part of the premium offering for popular DeFi news source The Defiant, and I guess we're going to see this kind of pay for access media more and more, in the crypto space and beyond. The ad-supported model is tough, so people are keen to move away from it, and a "freemium" model with some public offering and more for a fee is popular in other domains, like gaming.

One of the drivers of much analysis and reporting in the cryptocurrency space is edge. People value information that allows them to understand market phenomena better or faster than other participants and make the right moves at the most advantageous times. This kind of information can often fetch a good rate in the market when sold as a club good.

Any kind of paywall is however creating a huge barrier to many people who could otherwise benefit from an information resource. Levelling the playing field is one of the crypto aspirations I like, it's good that more people can learn about this stuff more quickly and that they don't have to invest money up front in resources to help them. There would be something sadly ironic about a crypto commons that is publicly recorded and accessible through distributed ledgers, but where the best accounts of what's going on and how it works are behind paywalls.

References

1. Harper, C. (2020). *People Are Tokenizing Themselves On Ethereum; Why "Personal Tokens" Raise Red Flags*. Forbes. https://www.forbes.com/sites/colinharper/2020/05/06/people-are-tokenizing-themselves-on-ethereum-why-personal-tokens-raise-red-flags/

2. *The Man Who Tokenized Himself Gives Holders Power Over His Life*. (2020, June 30). CoinDesk. https://www.coindesk.com/man-who-sells-himself-now-wants-buyers-to-control-his-life

3. *FC Barcelona's Token Sale Hit $1.3M Cap in Under 2 Hours—CoinDesk*. (2020). https://www.coindesk.com/fc-barcelonas-token-sale-hit-1-3m-cap-in-under-2-hours

4. *Lil Pump Is Doing a Social Token Called PumpCoin.* (2020, December 18). CoinDesk. https://www.coindesk.com/lil-pump-is-doing-a-social-token-called-pumpcoin

5. *Rapper Lil Yachty Sells Out Social Token in 21 Minutes.* (2020, December 10). CoinDesk. https://www.coindesk.com/rapper-lil-yachty-sells-out-social-token-in-21-minutes

6. Shreyas Hariharan (2020, November 21). *Social Tokens* https://shreyashariharan.com/2020/11/21/social-tokens/

Blockchain for What?

Cryptocurrency

> 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 verify that they are being enforced. It minimizes the need to trust other parties, greatly expanding the ways in which parties who do not trust each other can interact productively. Bitcoin's big wins 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 in order to have control of one's assets. Adherence to the rules can be verified on the blockchain, access cannot be restricted because of the network's distributed peer-to-peer nature.

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. The network benefits from many peers, and requires some minimum threshold in order to achieve meaningful global accessibility.

Bitcoin's phenomenal success so far indicates that blockchains are good for running a distributed ledger that tracks ownership and payments- i.e. a currency. The market and mindshare penetration achieved by a product that did not exist

11 years ago indicates that there is a demand for the service that Bitcoin provides. Bitcoin's more or less unspoiled record of enforcing its rules continually over the last 10 years has established credibility for blockchain as a means to operate a robust immutable censorship-resistant distributed ledger.

Software/Asset/Fuel/Network

A blockchain's infrastructure is made from FOSS and a public record shared by thousands of nodes, and so it is impossible for a single authority to exercise complete control over it. 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.

Conversely, this flexibility could cast doubt over a cryptocurrency's monetary policy, issuance schedule and supply cap. Any of the network's rules *can* change if there is consensus "at the social layer". Furthermore, miners *could* behave in ways which make the network depart from its social contract, as was suggested in relation to the Binance hack, where miners may have been offered a bounty to roll back the chain and edit one transaction. There is no definitive version of the social contract, and different people or groups may hold different views on how to interpret it in an unforeseen situation.

The discussion of any possibility that Bitcoin's rules may be altered is frowned upon by many who are cryptocurrency proponents, as the very act of discussing it serves to shift the Overton Window of acceptable discourse. When decision-making is informal it is enmeshed in the discourse. Discussion of an undesirable possibility, especially when the discussion is in neutral or accepting tones, increases the perception that this scenario may unfold. Public discussions may also serve to increase the likelihood that the hypothesized event will occur in the future. Everyone who reads these discussions is alerted to the possibility, some actors may seek to bring it about and some constituents may be persuaded that it represents an acceptable deviation from the social contract.

At the same time, open discussion of weaknesses can lead to ideas and approaches which address or mitigate them. This is in essence a conundrum of whether to embrace the adaptable FOSS nature of blockchains and improve iteratively, or to reject adaptability as dangerous and instead seek ossification, promoting the characterization of cryptocurrency as an asset or commodity.

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 forks and threatened forks of 2017, Bitcoin's social contract seems to be more stable too, now that the "big blockers" have departed.

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)[1] or exploiting an opportunity to profitably deviate from the established social contract (e.g. double spend attack reorgs).[2]

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.

In 2020, Jesse Walden wrote about progressive decentralization[3] and offered a playbook for building crypto applications by establishing market fit, growing a community that can maintain the resource, and only then aiming to achieve sufficient decentralization.

Commons-based Decision-making

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)[4], 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. 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 Bitcoin 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 utility. 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 experiments 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. In these cases the aim is to delegate some decision-making power to a prediction market driven entity that is paid to help find the "right" decisions.

The essential aim of decentralizing decision making power is to address the weakness 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 their 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 buy 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. And sometimes Voice is the domain name that $30 million of ICO investors funds got spent on.[5]

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).

Governments on the Crypto Commons

Estonia has been pushing the boundaries of the "digital state" for some time, and part of their offering to citizens now relies on a blockchain-type system. This is not a public blockchain powered by PoW consensus like Bitcoin, but rather an alternative permissioned system which actually pre-dates Bitcoin. One key benefit derived from this blockchain-type system is that it is not possible to change data quietly. Data is not immutable as it would be in a cryptocurrency, but rather there are strict controls on who can access and update the data, and this cannot be done without leaving a trace.

All Estonian citizens have a Digital ID which they can produce electronic signatures with, and this forms the basis of their interactions with the state, but also some private companies. Online banking in Estonia uses this Digital ID and did not have to come up with its own method of authenticating users.

X-Road is the system that connects many data sources together and allows people to make queries about the data associated with an individual's Digital ID across independent systems based on their permissions. Data is owned by the individual citizens that it relates to, and crucially access to this data is logged and attributed to the IDs of the accessors.

The system allows for much swifter and easier access to the data about an individual, and could easily become a tool of surveillance. It is therefore important that reads of the data are logged, and this is a key feature of the Estonian e-health system.[6] The owner of the data can see a record of who else has accessed it and question any illegitimate access, there are strict rules and penalties for unwarranted access to a patient's medical data.

A comprehensive report[7] by the UK Government's Chief Scientific Adviser in 2016 also saw great potential in blockchain technology for transforming the delivery of public services, including reduced cost of operation and fraud, greater

transparency of transactions between government agencies and citizens, greater inclusion of people who are on the fringes of the financial system and reduced costs of protecting citizens' data. Importantly, this report sees a major role for digital currency applications, along with potential in new forms of contract and new ways to build applications. Unfortunately the report does not seem to have been followed up with any significant action.

In Oct 2019[8] "Chinese President Xi Jinping said China must make 'greater effort' to develop and apply blockchain technologies and gain an 'edge over other major countries'." This is, unsurprisingly, not an embrace of Bitcoin (which is "not entirely banned")[9] but the underlying technology, which the Chinese government is quickly moving to deploy and test. In 2020 the Chinese Central Bank Digital Currency (CBDC) made quick progress towards an initial test in Shenzen in April[9] and by November they were scaling up with an airdrop[10] distributing $1.5 million to residents of Shenzen through a lottery, with thousands of retail outlets equipped to receive payments. China is also developing a Blockchain Service Network [11] which seems to be aiming to facilitate smart contracts.

A group of 7 central banks together with the Bank of International Settlements have published a report[12] setting out foundational principles of CBDCs and what the minimum requirements are to adopt one. The Central Bank of the Bahamas is first to market with a fully deployed CBDC with the launch of the Sand Dollar.[13]

The European Central Bank is talking about a Digital Euro, and in Oct 2020 published a major report on the subject.[14] This is just the beginning of a long process for the Eurozone however, a decision is expected in mid-2021 on whether to proceed with the design of a digital euro.

It remains to be seen whether these CBDCs and other government-backed blockchain efforts will be commons based or decentralized in a meaningful way. They will have open source software and distributed ledgers, but they may also have special keys for the admins to tweak settings (like your balance).

For other governments "being on the crypto commons" is about availing of the censorship-resistance to bypass sanctions and the payment providers who aren't allowed to deal with them. Venezuela has gone from cracking down on Bitcoin miners to mining the asset itself[15], and Iran is formulating a national strategy[16] for its emerging crypto mining industry, which already accounts for 4% of global BTC hashrate according to the Cambridge Bitcoin Electricity Consumption Index.

References

1. *Report: "Wrapped Serials" Attack. - By PIVX Core Developers | Medium.* (2019). https://medium.com/@dev.pivx/report-wrapped-serials-attack-

5f4bf7b51701

2. *Once hailed as unhackable, blockchains are now getting hacked.* (2019). MIT Technology Review. https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

3. Walden, J. (2020, January 9). *Progressive Decentralization: A Playbook for Building Crypto Applications.* Andreessen Horowitz. https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management/

4. Szabo, N. (2017, February 9). Money, blockchains, and social scalability. *Unenumerated.* https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

5. Biggs, J. (2019, June 19). *Block.one Paid $30 Million for a Domain.* CoinDesk. https://www.coindesk.com/block-one-pays-30-million-for-a-domain-name

6. Halim, S. (2019, January 11). Learning from the Estonian e-health system. *Health Europa.* https://www.healtheuropa.eu/estonian-e-health-system/89750/

7. Chief Scientific Advisor. (2016). *Distributed Ledger Technology: Beyond block chain.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

8. Wood, C. (2019). *China goes bullish on blockchain.* Business Insider. https://www.businessinsider.com/china-bullish-on-blockchain-xi-jinping-2019-10

9. *China Didn't Ban Bitcoin Entirely, Says Beijing Arbitration Commission.* (2020). Cointelegraph. https://cointelegraph.com/news/china-didnt-ban-bitcoin-entirely-says-beijing-arbitration-commission

10. *$1.5 million of China's CBDC Will be Distributed in Shenzhen—Decrypt.* (2020). https://decrypt.co/44410/1-5-million-of-chinas-cbdc-will-be-distributed-in-shenzhen

11. *China's Blockchain Service Network Integrates Chainlink Oracles.* (2020.). Cointelegraph. https://cointelegraph.com/news/chinas-blockchain-service-network-integrates-chainlink-oracles

12. BIS. (2020). *Central bank digital currencies: Foundational principles and core features.* https://www.bis.org/publ/othp33.htm

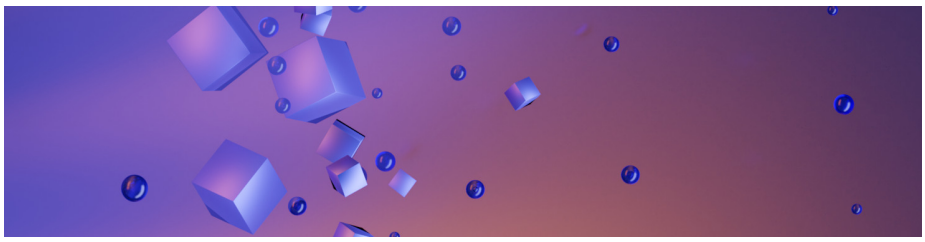
13. *Central Bank of Bahamas Launches Landmark 'Sand Dollar' Digital Currency.* (2020, October 21). CoinDesk. https://www.coindesk.com/central-bank-of-bahamas-launches-landmark-sand-dollar-digital-currency

14. European Central Bank (2020, October 8). *Report on a digital euro.* https://www.ecb.europa.eu/euro/html/digitaleuro-report.en.html

15. *Venezuela's Socialist Regime Is Mining Bitcoin In a Bunker to Generate Cash.* (2020). from https://www.vice.com/en/article/k7a3j3/venezuelas-socialist-regime-is-mining-bitcoin-in-a-bunker-to-generate-cash

16. *Iranian President Calls for National Crypto Mining Strategy.* (2020, May 21). CoinDesk. https://www.coindesk.com/rouhani-bitcoin-mining-iran

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 contrib-

utors 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.

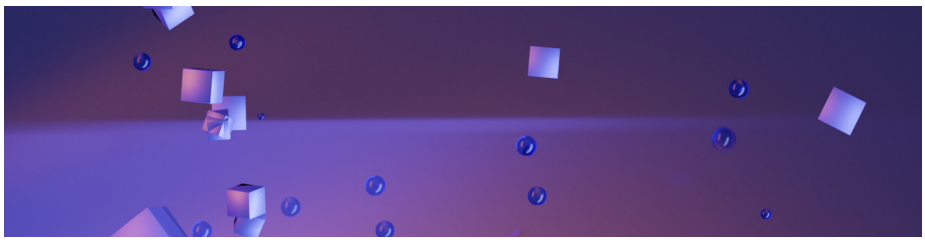
This is a novel funding mechanism for commons-based peer production, which outside the domain of FOSS has been even more hampered by the difficulties of funding the production of public goods.

DAOs are an effort to build methods of coordination into the commons, they are commons-based 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).

So far however this potential is a distant possibility, with clunky user experience, flawed structures, and high transaction fee costs have limited most of the DAOs which have been created so far to the status of curiosity or failed experiment. Popular DAO forms are all about allocating capital or funding, when they work well they are like more elaborate multi-sig wallets.

DAOs for looking after blockchain networks, where they are endowed with ongoing block rewards, inherit the longevity of their blockchains. Where there is a significant flow of funding, you can be assured there will be at least some people around to allocate and claim it. The only outright failures occur 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, but I'm still waiting to see what that kind of success looks like.

Broke Media, Shaky Platforms



Our software infrastructure for handling data is poor and the security of our information is weak, 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.

In 2020 we also saw platform operators getting more overtly involved in politics, with twitter putting disclaimers in front of many of Donald Trump's tweets[1]. We also saw international disputes over the control of platforms and which platforms a nation's citizens are using, with efforts to ban Chinese owned platforms like TikTok and WeChat from the US.[2]

The perils of a monopolistic mass media have been well described as long ago as the 1980s, by among others Herman and Chomsky in Manufacturing Consent [3]. In the 2000s we saw much experimentation in communications and many new forms of web based interaction and content production took off (Web 2.0). The web, and then social media, were greeted with enthusiasm by many because they would democratize the production of news and other media. We saw mass adoption of some of these new platforms, as a species they changed our behaviors and opened up new possibilities. Now we are seeing more of the problems with the way these platforms were designed, and a year when people have spent more time online than ever before is speeding up that process.

2020's big banking scandal was the FinCEN Files, which involved 2,657 leaked documents being shared with journalists. These were mostly mostly "Suspicious Activity Reports", where a transaction is flagged as looking suspicious by the bank according to some criteria. The point being made in most of the stories about these leaked documents is that the banks and authorities aren't doing anything even once the transactions are marked as suspicious. There were plenty of other banking scandals[4] too of course, including Goldman Sachs confessing to "conspiring to violate the Foreign Corrupt Practices Act (FCPA) with a scheme to pay over $1 billion in bribes to foreign officials in exchange for underwriting approximately $6.5 billion in bond deals for a Malaysian Fund, 1MDB." Goldmans' shares rose 1% on the news that they would not be prosecuted at this time. They're off the hook as long as they cooperate with ongoing investigations, and they already promised to do better next time!

It seems to me that the global anti-money-laundering system is pretty ineffective and likely corrupt, judging by the number of scandals involving banks turning a blind eye to their clients' murky dealings. I'll put my *not an expert* disclaimer out here and say that it looks to me like laundering the money is just part of the game now for organized crime. Giving responsibility for detection of crime proceeds to banks, who are the same entities that make vast sums from servicing these clients, is inviting corruption.

Broke Media

The new media landscape is characterized by information overload, with a bewildering array of sources to choose from and a dominant business model that sells users' data and access to their feed so that the buyers can try to modify the behavior of the platforms' users. This puts the social media companies in a position where they are not good custodians of what is effectively a public-produced resource - users do the work to add value, the company tweaks settings to maximize the value which can be extracted. Given this context, making the same companies more responsible for moderating the discourse on their platforms is problematic, it's asking them to exert even more influence, and in more specific ways.

To me this seems like the wrong direction to be headed in. Top-down content moderation policies are easily used as tools for manipulation by people who manage their implementation - unless accountability is carefully built into the system. Instead, we might consider reducing our reliance on the companies who provide these new communications platforms, and consider how we might build and maintain equivalent platforms as part of the digital commons. These spaces are part of the digital commons but we are presently entrusting their management and maintenance to the people who can hook the most users for the longest time and make the most money from advertising to them and changing their behavior - and pump their stock price the most in the process.

Hard Software

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. The question of how a a developer community engages with a large population of users of their software is still being explored but we can at this stage conclude that "through the hierarchical organization of a multinational corporation" is not a great answer.

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.

References

1. Twitter hides Trump tweet for 'glorifying violence'. (2020, May 29). *BBC News*. https://www.bbc.com/news/technology-52846679
2. Lerman, R. (2020). TikTok creators successfully block U.S. app ban with lawsuit. *Washington Post*. https://www.washingtonpost.com/technology/2020/10/30/tiktok-ban-halted-injunction/
3. Herman E. S. & Chomsky, N. (1988). *Manufacturing Consent*. Vintage.
4. *2020's Biggest Bank Scandals*. (2020). https://finance.yahoo.com/news/2020-biggest-bank-scandals-130029494.html

At the Crypto Crossroads

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 more of an interest in blockchains. This is inevitable and I think there are two ways it could go broadly, we will likely see both happening for a while. The first is for established companies to make their own version of the it, the second is for them to find an area of the crypto commons to make their own, or terraform some portion of it to suit their needs.

Corporate Base Layer

Facebook has been the most visible proponent of building a corporate-backed blockchain payments network, with Libra (now called Diem)[1] receiving a frosty reception in 2019 when it was announced as a multi-currency stablecoin. After a year of discussions with regulators, Diem is now planning for a more limited launch of a dollar-backed stablecoin in early 2021[1] - the basket of backing currencies was one of the aspects regulators took exception to. A bill introduced in December 2020 [2] would require stablecoin issuers to secure bank charters and regulatory approval before releasing these - this is widely seen as a response to Libra and the threat of similar launches.

The Telegram messaging app ICO raised $1.7 billion[3] in private investment for TON tokens, but they were sued by the SEC for issuing unregistered securities, Telegram opted to give the ICO money back and pay a penalty[4] to resolve the matter.

We can anticipate that other corporations will learn from these events and manage to launch products without getting entangled with regulators. JP Morgan have already shown how to do it with their own JPM Coin blockchain toy for internal use, although that wasn't a very ambitious use case. By October 2020 JPM coin was being used for the first time [5] and the JP was setting up a unit with 100 staff members, described as "close to making money".

Corporations on the Commons

For corporations that don't have such grand ambitions as a blockchain of their very own, the question is whether they're interested and looking to carve out a space somewhere on the crypto commons.

Michael Saylor, CEO of MicroStrategy, a publicly listed company which has been on a Bitcoin buying spree in 2020[6], is one of the more interesting characters to emerge on crypto twitter this year. MicroStrategy announced in August that it was going to make Bitcoin its primary reserve currency to hedge against dollar inflation, and has since then bought 70,470 BTC, putting it one place ahead of the United States government as the fifth-largest holder of Bitcoin - although I don't think this considers that US Gov just added to its balance with a seizure of $1 Billion worth of Silk Road era BTC.[7]

Saylor was quickly adopted by many Bitcoin fans as a new champion who was preaching the message of escaping inflation with fixed-supply Bitcoin within circles where people have more money at their disposal and more weight to push the Bitcoin price higher if they add demand to the market. Saylor has reciprocated with poetry and tweets singing the praises of the Bitcoin Maximalists, and echoes their talking points. With more companies announcing Bitcoin positions, this seems to be a major catalyst driving Bitcoin's price to new highs.

Paypal is now offering Bitcoin for sale to its users,[8] but not allowing them to withdraw it or send it to each other, yet at least. A number of companies now offer similar "paper crypto" services like this where the customer is not really buying the asset but more like a "contract for difference" instrument from the seller.

The other big financial sector disruptor is Square Inc., and they have been even faster to embrace cryptocurrency, with a purchase of $50 million BTC in October 2020 [9] the latest in a long series of pro-Bitcoin moves from Square.

There are also a number of crypto-origins corporations that serve as a bridge between the legacy economy and crypto. In the ICO era that bridge was made of pre-sale deals which gave the fiat investors a preferable rate to enter the crypto pool at - the corporation may also have paid for liquidity that made it easier for the investors to dump their tokens at a profit. In 2020 we saw Uniswap evolve this concept as an airdrop and liquidity mining, where the tokens weren't being sold in an ICO but given to users - with 21% of those tokens going to the corporation and 18% to its early investors.

The combination of significant VC funding and a big role for the VC-backed entity 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. SushiSwap are have put this logic to the test by cloning Uniswap's code and creating a competitor built upon its shoulders - lacking the skilled contributors who wrote the code originally, but also buoyed by the absence of a requirement to give 40% of tokens to some corporation(s).

This way to the walled garden

Once the institutions are Bitcoin holders, and there's a version of Bitcoin which suits them, where do people go for p2p electronic cash? This could still be Bitcoin, at the margins, but there are some good reasons to think it won't be.

Exchanges won't except BTC from certain blacklisted addresses, and many of them retain the services of chain analysis companies who can tell them about any taint associated with incoming coins - I expect that over time it will become increasingly difficult to send coins which have been mixed to an exchange. The Lightning Network could provide a solution to use Bitcoin for regular p2p transactions, but it seems likely to remain fairly exclusive while the technical barriers are high and on chain fees for opening and closing channels are expensive. The privacy implications of transacting on LN are also just being explored.[10]

Reasonable privacy is a prerequisite to widescale self-custody and use of cryptocurrency. If people can easily find out how much cryptocurrency you have, it's not safe for you to have very much. In 2020 we are seeing the outline of this conflict emerging, a wall being built around "safe BTC" and the people you can get it from, with mechanisms in place that encourage leaving it in the custody of some company. This is the agenda of the people behind the new proposed regulation of transfers to "self-hosted" wallets.[11]

We are also (writing at the end of 2020) in the midst of a delisting of "privacy coins" from exchanges.[12] Blockchains that have some feature for protecting users' privacy are not being allowed on the same exchanges as assets with a transparent ledger where users transactions can be tracked more easily.

Bitcoin is being sanitised for the institutions, and the network's more powerful constituents are in the main happy to go along with this because the inflow of institutional capital is expected to drive the price of BTC up.

Walled garden bypass

On the other side are people building around whatever points of centralization they can find, developing infrastructure to deliver their vision of a decentralized [whatever]. If Decentralized Finance can replace financial intermediaries with smart contracts and reduce costs by increasing efficiency that's great, and doing it on an open accessible blockchain is even better. However, for me personally "decentralize finance", in the sense of aping the fiat financial system on a blockchain, is a fairly weak rallying cry.

Decentralized Exchanges of various forms are however proving themselves to be a useful addition to the ecosystem. Ethereum users have a variety of liquid decentralized exchange protocols with automated market makers to choose from now, and Decred has recently launched the initial version of DCRDEX, which is running on a client-server model for accessing order books, with traders then completing the trades directly on chain and the server standing by to ensure everyone follows the rules about following through with matched orders.

For every round of new regulation and legislation, there will be people looking for and finding workarounds and loopholes. With open source software they have a flexible medium to work with, and with an open internet connecting everyone the hackers are in a strong position now that the fundamentals of cryptocurrency are being demonstrated over time.

Nurture the Crypto Commons, so they grow up Big and Strong

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. These projects also thrive on attention and productive contributions, although they are susceptible to derailment and distraction.

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 [13] 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 both 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.

Public 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 likely be available in some capacity.

These commons-based digital organisms are going to have to compete with offerings from major corporations (who can leverage their assets in other domains, like social media) and national governments (who can mandate adoption), both of which could deploy significant resources and staff their commons with employees or contractors.

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.

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

References

1. *Libra Rebrands to 'Diem' in Anticipation of 2021 Launch.* (2020, December 1). CoinDesk. https://www.coindesk.com/libra-diem-rebrand

2. *US Bill Would Require Stablecoin Issuers to Get Bank Charters.* (2020, December 2). CoinDesk. https://www.coindesk.com/us-lawmakers-introduce-bill-that-would-require-stablecoin-issuers-to-obtain-bank-charters

3. *Telegram Doubles Amount Raised in ICO to $1.7 Billion.* (2018, March 30). CoinDesk. https://www.coindesk.com/telegram-doubles-amount-raised-in-ico-to-1-7-billion

4. Jaeger, J. (2020). *SEC seeks to thwart cryptocurrency masquerading as ICO.* Compliance Week. https://www.complianceweek.com/regulatory-enforcement/sec-seeks-to-thwart-cryptocurrency-masquerading-as-ico/27896.article

5. Son, H. (2020, October 27). *JPMorgan creates new unit for blockchain projects, says the technology is close to making money.* CNBC. https://www.cnbc.com/2020/10/27/jpmorgan-creates-new-unit-for-blockchain-projects-as-it-says-the-technology-is-close-to-making-money.html

6. *MicroStrategy buys the dip—Now has more BTC than US govt.* (2020). Cointelegraph. https://cointelegraph.com/news/microstrategy-buys-the-dip-now-has-more-btc-than-us-govt

7. Rooney, K. (2020, November 5). *Record $1 billion worth of bitcoin linked to the Silk Road seized by U.S. government.* CNBC. https://www.cnbc.com/2020/11/05/1-billion-worth-of-bitcoin-linked-to-the-silk-road-seized-by-the-us.html

8. McBride, S. (2020). *You Can Now Buy Bitcoin On PayPal For $1.* Forbes. https://www.forbes.com/sites/stephenmcbride1/2020/12/04/you-can-now-buy-bitcoin-on-paypal-for-1/

9. *Square, Inc. Invests $50 Million in Bitcoin.* (2020). Square. https://squareup.com/us/en/press/2020-bitcoin-investment

10. Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., Miller, A., & Meiklejohn, S. (2020). An Empirical Analysis of Privacy in the Lightning Network. *ArXiv:2003.12470 [Cs].* http://arxiv.org/abs/2003.12470

11. *Self-Hosted Bitcoin Wallets Become Front Line in Fight Over Crypto Regulations*. (2020, December 18). CoinDesk. https://www.coindesk.com/self-hosted-bitcoin-wallets-become-front-line-in-fight-over-crypto-regulations

12. *Privacy Coin Advocates Persevere Amid Exchange Delistings*. (2020, December 11). CoinDesk. https://www.coindesk.com/privacy-coin-advocates-crypto-exchange-delistings

13. Monegro, J. (2019). *Sovereign Cryptonetworks*. Placeholder. https://www.placeholder.vc/blog/2019/7/31/sovereign-cryptonetworks

Conclusion

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

- The blockchain space is worth watching if you're interested in commons-based or digitally native means of production.
- We should all be interested in commons-based production, because phenomenal resources (e.g. Linux, Mozilla, Apache, Wikipedia, Stackoverflow) are being produced in this way (efficiently, at low cost) and being made freely available. Contrast this with the level of value *extracted from* resources like social networks, which are also "peer produced" in the sense that the valuable content comes from the users, but are far from "commons-based".
- Bitcoin and other public blockchains are pioneering early examples of robust networks/services being established on the commons, "owned" and operated by the peers (network nodes) in a decentralized manner with no centralized points of control and no off switch.
- Commons-based peer production and common pool resources are useful lenses through which to observe the blockchain 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. How well the various constituencies involved in "producing" a blockchain are aligned, and the degree of friction in their interactions, will be significant factors in determining the course the project takes in the long run.

- 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