# An economic theory of blockchain foundations

Darcy Allen, Chris Berg, Sinclair Davidson, Trent MacDonald, Jason Potts

RMIT Blockchain Innovation Hub, RMIT University, Melbourne

contact author: jason.potts@rmit.edu.au

RMIT BIH WORKING PAPER - 9 May 2021

**Abstract.** Blockchain (or crypto) foundations are nonprofit organizations that supply public goods to a crypto-economy. The standard theory of crypto foundations is that they are like governments with respect to a national or regional economy, i.e. raising a public treasury and allocating resources to blockchain specific capital works, education, R&D, etc., to benefit the community and develop the ecosystem. We propose an alternative theory of what foundations do, namely that the treasury they manage is a moat to raise the cost of exit or forking because the benefit of the fund is only available to those who stay with the chain. Furthermore, building and maintaining a large treasury is a costly signal that only a high quality chain could afford to do (Spence 1973). We review these two models of the economic function of a blockchain foundation - (1) as a private government supplying local public goods, and (2) as a moat to raise the opportunuty costs of exit. We outline the empirical predictions each theory makes, and examine the implications for optimal foundation design. We conclude that foundations should be funded by a premine of tokens, and work best when large, visible, transparent, rigorously managed, and with a low burn rate.

Keywords: blockchain foundations, public goods, crypto economy, costly signalling

# 1 How to study blockchain foundations

All economies face the problem of how to provide public goods. In the crypto-economy, this is the role of blockchain foundations (a.k.a. crypto foundations). In economic theory, public goods are defined as goods that are non-rivalrous and non-excludable (Samuelson 1954). The implication of goods with these properties is market failure, i.e. markets will fail to provide them (at socially optimal levels). If such goods are to be provided in a competitive economy, then they will require an alternative institutional mechanism. In a nation state economy, that mechanism is government provision, usually publicly financed through compulsory taxation.[1] As such, governments provide public goods across a range of physical and administrative economic infrastructure because markets will often fail to do so.[2]

Blockchain foundations are to a digital blockchain economy, *mutatis mutandis*, what governments are to a real physical economy, namely institutional mechanisms to endogenise externalities through the provision of high-quality social welfare maximizing public goods.[3] These foundations are solutions to the problem of market failure in the essential provision of public goods at the base layer of an economy. In this way, the economic theory of public goods and public finance provides an obvious starting point for analysis of blockchain foundations.

Layer one (L1) blockchains build economies, but they do not have governments; instead they have foundations. Some foundations are in place before mainnet launch, others roll out duing the bootstrap phase, or gradually as the network grows. Almost all large blockchain projects have a foundation, which is an arms-length not-for-profit organization, created by the founding team, but with separate governance, and tasked with providing public goods related to the security and development of the blockchain's ecosystem. However, because subjects can exit to another blockchain or other jurisdiction, the goods these foundations provide are strictly speaking actually *local public goods* (Tiebout 1956),[4] or *club goods* (Buchanan 1965). The economic theory of competitively provided public goods and club goods are useful and powerful frameworks for the economic analysis of blockchain foundations.

---

[1] Public goods in a nation state can also be funded through monetary means due to the Sovereign monopoly over money (i.e. a legal tender, as a medium that is accepted in settlement of a debt, public and private), through increased issuance of a fiat currency, i.e. seigniorage, which is a actually a form of *inflation tax*.

[2] On the economic theory of the private provision of public goods, see Bergstrom et al (1986). On the use of blockchain technology to coordinate the private provision of public goods, see Nair and Sutter (2018).

[3] Nation state governments also seek to provide digital public goods such as: software, standards, data (OECD 2020). Crypto economy (local) public goods overlap with this set, but are more specific; security, protocol development and maintenance, and code fixes.

[4] Tiebout's (1956) conception of local public goods was a theoretical response to Sameulson's model of public goods extended to competitive provision of public goods in a federalist context (also called 'foot voting'). Buchanan's (1965) model of club goods introduced the idea that many goods that were thought to be public goods were actually excludable (e.g. a 'public' swimming pool with a fence and gate) and that these were public goods only for a particular community that was permissioned to access those goods or receive those benefits (and, symmetrically, to incur the costs of provision). Blockchain infrastructure has clear public good-like properties, but because in many instances there are competitive exit options (to another blockchain) or possibilities for exclusion (through permissioned access, or access through an L1 token), then strictly speaking these are local public goods or club goods rather than public goods *per se*.

## 2 What are crypto foundations?

Many blockchain projects have evolved or spun-out organizations or programs, generally called foundations. The primary role of these foundations is to distribute funds to support the development of public goods infrastructure for the protocol. On L1 blockchains there are many examples of well-developed foundations (such as the Bitcoin Foundation, the Ethereum Foundation, the Algorand Foundation, the Vechain Foundation, the Cosmos ecosystem's Interchain Foundation, the Zcash Foundation, the Tezos Foundation, and the Cardano Foundation). On layer two (L2) protocols and applications there are an increasing number of large treasuries governed as either formal or informal foundations (such as the UniSwap Grants Program and the Compound Grants Program). Because blockchai projects (L1 and L2) are build to serve a growing community of users, the foundation is the institutional mechanism to provide public goods to that community.

Blockchain treasuries are vaults of cryptocurrency tokens (either of a protocol's native token, or in the case of some defi protocols, of a Layer 1 settlement token such as Ethereum). The dominant model for stocking these treasuries is through a 'premine' of tokens, where developers mint the total stock of tokens at the launch of the network. Some of these tokens are sold or airdropped, some are held by the development team, and some are placed in the treasury to support the future development of the network and public goods provision.

Blockchain foundations exist to solve the operational problem of how to distribute treasury funds. Formal, legal entities structured as foundations are not the only way to distribute treasury. For example, for those blockchain protocols and applications that allow token-holders voting rights, a common approach is to distribute public goods funding solely through a direct democratic vote of token-holders. This we can describe as direct governance by a decentralised autonomous organisation (DAO). Direct DAO governance over a treasury often evolves into formal foundation governance. In other cases, either a single individual who holds the private key to the treasury wallet is the sole decision-maker concerning treasury distribution (with obvious public choice implications, see Berg 2021). A crypto foundation provides, from an operational or instrumental perspective, a range of public goods to its protocol ecosystem.

Let us briefly review the stylised facts under consideration about crypto foundations: i.e. what they are, what they do, and how they do it. This is useful to make clear their role as government-like administrative bureaucracies, and to consider the extent to which we can understand crypto-foundations as 'private governments' for emergent digital economies.

First, the organization of foundations is usually as an arm's length fund, with a separate board to allocate resources to various projects. Most operate on a mixed model of supporting a core team of codebase developers, plus a grants program, with community members proposing projects over a range of topics and awards. While it is in theory possible for a crypto foundation to be for profit, in practice all crypto foundations so far observed are non-profits (i.e. can receive donations). The charter of these nonprofit organizations is always, with varying degrees of explicit formulation, to support the development of the

protocol ecosystem. Blockchain foundations often have a *manifesto* and a clear mission, which reflects the culture of the underlying chain.

Second, they often have a *corporate structure*, including an executive board with various advisory boards (technical, educational, economic, etc). This corporate form then undertakes a range of tasks decided by the board. Foundations typically will fund and support the running of conferences, blogs and sponsorship. They will hire or otherwise support developers to work on the codebase, deal with support, and fix bugs and perform essential maintenance. This is a particularly critical function and one the open source community has long struggled with (Eghbal 2020). Importantly, foundations fund blockchain specific research, often running grants programs and hackathons. The Ethereum foundation, for instance, is 'dedicated to supporting ethereum and related technologies'. They are like industry associations, but for a chain ecosystem, and so provide club goods. They are like governments, in providing public goods.

Third, blockchain technology evolved from the *open source community*, and the development of open source has a long history of using foundations as an organizational governance model for the various projects (e.g. the Linux foundation) (Learner and Tirole 2002, 2005, Eghbal 2020). Blockchain foundations appear to have been explicitly modelled on open source software foundations.[5] It remains a task for further research and historical investigation to examine the pathways by which specific instituional forms and cultural norms were copied across. Foundations are useful vehicles when dealing with the need to provide effective governance of a common pool resource (e.g. the codebase), while making high-quality decisions about the development of that digital (i.e. non-rival) resource, including the allocation of effort from volunteers who seek to work on this. The basic challenge in the open source community is that the economic development of a zero-price open-access asset - i.e. an information good (Ostrom and Hess 2003) - means that market-based allocation mechanisms are likely to fail, and the absence of employment contracts due to reliance on volunteers and donations means that a model of hierarchic decision-making in a firm is also likely to fail. The economic infrastructure of a for-profit development will likely be inefficient for the provision of common pool resources, and especially knowledge commons (Ostrom 1990, Frischmann et al 2014, Potts 2019). Hence a foundation, with its particular structure of shared ownership and governance, can resolve some of the missing incentives.

Fourth, a foundation has one other obvious advantage, namely *tax efficiency*. It is noteworthy that many crypto foundations are chartered as not-for-profit organizations, creating a tax-minimizing corporate entity that is publicly transparent and with clear governance that is distinct from the various for-profit enterprises and ventures that will be built upon it. Similarly, many foundations are based in tax advantaged jurisdictions. For example, the Interchain Foundation and the Ethereum Foundation are headquartered in Zug, Switzerland. This supports a tax efficiency thesis for the existence of foundations, i.e. in a world with zero taxes, there would be no reason for foundations to exist. But a tax efficiency

[5] Hackerspaces and makerspaces have a similar heritage from open source software (Williams and Hall 2015), but dealing with shared hardware (e.g. 3D printers, CNC mills, etc) as well as pooling and sharing tacit craft knowledge, both of which are innovation infrastructures as common pool resources (Potts 2019).

model also has the property of public transparency and accountability (to qualify for non-profit status), which depending on perspective may be considered a cost or a feature.

Fifth, a foundation can also play a key role in facilitating *decentralisation* of a blockchain protocol or ecosystem. Blockchains are born centralised (Allen and Berg 2020) - a founder (such as Satoshi Nakamoto in the case of Bitcoin) or founding team must build and launch the protocol. However, the ongoing security and viability of the blockchain relies on achieving a credible level of decentralisation. This can be achieved in different ways (e.g. airdropped tokens, public blockchain, a staged transition, etc.), but an independent and well-funded foundation with a strong mandate and professional governance is a clear signal to the market about a blockchain's institutional commitment to the values of decentralization and to the operational requirements of its ongoing process. The distribution of treasury funds can shape the process of decentralisation. For instance, treasury distribution that only supports founders or a small group of insiders will invariably result in less decentralisation than when the funds are more distributed widely. Of course, the benefits of a narrow and more targeted distribution (i.e. against decentralisation) accrue to the possibility of both patronage (a benefit to those both giving and receiving) and efficiency due to allocating decision-making power to those judged to have specific or desirable competences or capabilities. This is a general problem with all democratic decision making, namely that the benefits from extending the franchise (more democracy) trade-off against the inivitable growth of low information and expressive voters (Buchanan and Tullock 1960).

Data from Crunchbase, combined with desk research, suggests that there are well over 50 foundations, all seemingly registered as non-profit organisations (USA, Switzerland and Singapore are heavily represented, but also Canada, Germany, Korea, as well as various tax havens). These are predominantly layer 1 blockchain foundations. They all have similar governance structure and functions:

- elected board, committee structures, voting mechanisms,
- a public website with charter and resources,
- semi-public discussion mediated through community-specific internet based channels,
- in-real-life meetings that align with conferences and events,
- calls for proposals for grants to supply research or other projects desired by the community
- serious concern with the quality of organizational governance, community representation, diversity, accountability, etc.

Most foundations post-date the mainnet launch of the blockchain, with many registered between 2014 and 2017. Most have representation from founding team developers, but are run by hired professional directors (remunerated through various schemes) and with expert and trusted community participants. On the face of it, and with only a few anomalous exceptions, layer 1 blockchain foundations all appear trustworthy, serious, and professional.

The structure of layer 2 foundations is less mature, reflecting the more recent development of significant treasuries in layer 2 protocols. Of the top four decentralised

finance protocols by treasury size,[6] three (Uniswap, Compound, and SushiSwap) manage their public good grant programs with a small committee of prominent individuals. At time of writing, the number three protocol, Aave, is also likely to adopt a similar structure.[7] In contrast to the mature layer 1 blockchain foundations, these committees lack legal identities, have limited formal governance structures, are not run by professional directors, and are more generally ad hoc. Even more so than the layer 1 foundations, these committees are filled with prominent and trusted community participants.

**Goals of Crypto Foundations**

The main objectives of these crypto foundations are explicitly stated on their websites, charters, or various vision statements and manifestos. These are similar to the stated public goals of open source software foundations, in that the core resource that the foundation is serving is the working codebase and the mission of the foundation is to support and grow that through various avenues and channels. An important distinguishing feature of layer 2 foundations is that they tend to have been explicitly endorsed by token holders through a token holder vote. Their 'constitution' is the original proposition to the DAO.[8]

Overall, the goal of the foundation is to provide governance and support to the shared community infrastructure. These roles (can) include:

- Codebase repository and maintenance, and core protocol development (supporting L1 developers)
- Product development to help grow the network (supporting L2 developers and those who are building within the protocol's ecosystem)
- Education and university programs
- Marketing, public relations and events (sponsoring/hosting conferences)
- Lobbying and political engagement
- To facilitate the ongoing process of decentralization

Some operations fit across several of these functions, for instance supporting hackathons, which are both education, product development. These roles broadly map to the public goods functions of a government, with respect to supply of base layer economic infrastructure and other market supporting and development investments (education, R&D, industry coordination and development, etc). Nation state governments also undertake defence and security, and law and order as foundational roles. However, in a blockchain network security is provided by the token consensus model and funded through the incentives built into the token reward. Buterin (2021) argues that this capital allocation between proof-of-work spending on network security, which is about 30 times more than is allocated to R&D, 'is a massive misallocation of resources' from the perspective of spending on public

[6] https://open-orgs.info/
[7] https://governance.aave.com/t/arc-aave-community-grants-program/3642
[8] See, for example, the proposal to the Compound Finance DAO for a Compound Grants Program https://compound.finance/governance/proposals/40 which was passed in March 2021.

goods from the perspective of the blockchain ecosystem versus the spending allocatio of the foundation (which does not allocate specific spending to network security).

**Financing Crypto Foundations**

From the perspective of public finance, there are two broad classes of blockchain foundation - donor based or premine based - from the perspective of funding model, which roughly corresponds to whether or not there was a significant premine to stock the treasury. The donor model is in effect funded by voluntary taxes, usually levied on 'whales', and in this sense is an extremely progressive taxation system. The premine model is in effect a species of seinorage, but with the inflation tax all occuring at or before t=0, and is thus expected inflation. Because there was no 'premine' in Bitcoin[9] the Bitcoin foundation relies entirely on donations, both financial and in-kind. Some foundation funds are actually stable coalitions of contributors.

The Ethereum and Algorand foundations, on the other hand, have treasuries established largely due to coins allocated from the premine. Most L1 foundations are funded through premines, and indeed, part of the purpose of a premine is to stock a treasury for a foundation. The institutional logic of this is that unlike a nation state that can restrict its citizens ability to exit the system, which facilitates taxation based public finance, a blockchain is a voluntary organization, and can only rely on voluntary contributions toward public goods, i.e. volunteering time and donations to the treasury. A blockchain protocol is in many ways a community that is jointly creating a common pool resource. This is a model that works reasonably successfully in many aspects of open source software and other parts of the internet that make use of community governance norms to guide and shape expectations of participation (Raymond 1999, Benkler 2006). This internet culture has successfully carried over to the crypto-economy, although with some innovations, such as the outsized role of conferences, t-shirts, social media, and memes.

# 3 Foundation as exit moat

Are these treasuries and their operations an efficient mechanism for the financing and delivery of (protocol specific, i.e. local) public goods? A common view is that the answer is broadly 'No', and that there is a massive misallocation in which the treasuries of L1 protocols, or more specifically the rate of spending, is orders of magnitude too small in order to support the provision of a socially efficient level of protocol infrastructure and public goods. This argument has been championed in a recent essay by Vitalik Buterin (23 March 2021) who noted:

> "The organisms that are the bitcoin and ethereum ecosystems are capable of summoning up billions of dollars of capital, but have strange and hard to understand

[9] Or, rather, the premine was conducted entirely by Satoshi Nakamoto, with those funds remaining locked and presumably under Satoshi's control - such that they may or may not reveal themselves to be a public goods treasury in the future. These are perhaps 'probabilistic public goods'.

> restrictions on where that capital can go. Clearly, this expenditure pattern is a massive misallocation of resources." (Buterin 2021).

In recent years Bitcoin has allocated about US$15 billion to funding network security (PoW) but just $20 million to R&D (i.e. 0.1% of 'public spending'). Ethereum and other L1 public chains have similar levels and ratios. In comparison, most industrialised nations spend about 2-4 percent of GDP on R&D. Buterin's point was that there is a missing force in this equation, and that to understand this imbalance one needs to appreciate the role of *legitimacy* in the power of the community to furnish public goods when needed.

**The costly signalling or 'exit moat' theory of crypto foundations**

However, we propose an alternative view of the nature and role of crypto foundations in which they are less 'Treasuries to fund public goods' but instead serve as an explicit and prominent exit cost to anyone who leaves the ecosystem or seeks to fork the chain.

A large, well-funded foundation is certainly a treasury and mechanism to supply public goods, but the public goods it funds are benefits to present network users, whereas an unspent treasury is a benefit to future network users. Therefore a large unspent treasury, or one that is designed to have a low and slow payout (of grants, etc), represents an exit tax to current network users considering either exiting the chain or forking the chain. This is the theory of 'foundation as forking insurance'. Our basic argument is that a large, visible but high transaction cost (to slow the burn rate) fund is a strategic barrier to exit.

By creating network stickiness, as well as mutual expectations of the opportunity cost of exit, and therefore confidence in investments in building on a particular chain, an exit barrier is a feature for many users, and especially for founders. If, on the other hand, forking or exit costs are low, such that any one or any subcommunity can easily leave, this creates a hazard of unstable expectations about complementary investment and network effects. For this reason, some exit frictions are desirable in order to create conditions for the safe alignment of mutual expectations about future participation, contribution and growth. A large treasury that cannot be accessed if a user exits is one such mechanism.[10] Somewhat costly exit, subject of course to functional governance and technology, is a feature from the perspective of the median user because it implies an expectation of costly exit for the many others, not only of oneself, thereby stabilizing expectations about the prospective behavior of those others.

The problem with using taxes to fund public goods is that they create a forking incentive to avoid the taxes, such that in a crypto economy, and ignoring network effects, you can exit at low cost to avoid any taxes (i.e. fees) that you don't want. The low cost of exit is a feature from the perspective of users/citizens, as it fundamentally limits the ability of the 'sovereign' to extract arbitrary rents or taxes. Competitive federalism has the same nice property in a territorial economy, such that the cost of exit imposes a ceiling on extractable rents through corruption. But the other side of this coin is that with arbitrary low exit costs,

[10] Observe that nation states do this with migration barriers, or by incentivising land or fixed asset accumulation that cannot be transferred, or by encouraging debt.

the ability to raise a capital pool to finance public goods is also profoundly limited. This is why Buterin (2021) emphasised the importance of perceptions of legitimacy to rally a community's resources, or to encourage donations (i.e. voluntary taxes).

In this context, a large, auditable, observable treasury is an artificial (designed) barrier to exit. At present, it is imagined that there are no barriers to entry and exit on a blockchain. To be sure, a successful fork requires that the 'dissidents' take the community with them (and so continue to benefit from network effects). This freedom of entry and exit also implies that there is a limit to arbitrary taxation and tribute in a crypto economy (due to the possibility of exit through forking). But freedom entry and exit could also generate unstable trading conditions within a blockchain ecosystem. As such, a mechanism that can reduce the propensity and likelihood of exit can be value adding, and one such mechanism is to have a large opportunity cost associated with exit. This is a role that a foundation can play, as a large fund that is available to access or receive benefits from only if you stay, but is no longer available if you exit.

We think this offers a useful explanation for why crypto foundations exist, and why they have the particular properties they have, namely that they are disincentives to exit. Note, of course, that this property is an evolutionary selection model of foundation fitness (Alchian 1950); it does not matter at all whether foundations were deliberately strategically designed with this feature in mind, or whether it was entirely accidental and unintended. What matters is the effect of the foundation on the behavior of the community of users and other stakeholders.

# 4 Discussion

**Predictions of our theory**

The 'foundation as mechanism to fund public goods' theory predicts that the size of a foundation is proportional to expected public goods needs, and that disbursements should be targeted and efficient. It particularly suggests that foundation funds will be spent.

In contrast, our 'foundation as exit moat' theory predicts that treasuries should be large (in order to create an explicit opportunity cost), with high public profile and transparent (in order to minimize ambiguity about that cost).

There are manifest benefits to the signalling equilibria from the fund being very public and on display. Our moat theory also predicts that disbursements should be small and slow, and that governance should be high-quality and excessively procedural in order to facilitate trust in the process, but to ensure that the treasury remains largely unspent. Furthermore, our moat theory predicts that clear signalling of manifest intention to make large disbursals *in the future* should be observed. An immediate implication is that our theory implies an optimal sized foundation, such that above a particular size is wasteful but any smaller gives weak incentives to stay - and with an optimal disbursement rate to maintain this balance. These predictions are broadly consistent with stylised facts.

Foundations are very new and are still in many cases controlled by small insider coalitions. This is a stable equilibrium, as centralised decision making is valuable in this context, and a purely democratic fund would likely soon be raided for consumption (Davidson 2021). Davidson argues that foundations will be characterised by concentrated control where insiders are highly incentivised by concentrated holdings of the native token but will also be non-profit organizations with strict limitations on the ability to distribute tokens to insiders. This argument builds on the initial insights of Hansmann (1990) that suggests that the non-profit form of organization is particularly well-suited for high-technology firms and for the provision of public goods. In the instance of blockchain foundations, they are both high-technology providers and provide public goods.

But minimizing the spending of the fund also limits the benefits from public goods supplied earlier rather than later. There is value from disbursement in terms of public goods. But running down the fund also implies risks of forking or exit. A large low dispersal foundation is in this way an implicit threat against potential coalitions of stakeholder exits.

**A foundation is a costly signal**

A foundation is a treasury, which has utilitarian purposes: to fund development of public goods. But a foundation is also a signal, a message, and for it to work it needs to be a true and honest (i.e. unfakeable) message, in the form of a *costly signal* (Spence 1973).

In this application of the costly signalling model (a branch of information economics), the decision to join or build on a blockchain is a type of *investment under uncertainty*, and the quality of a blockchain is subject to *asymmetric information*. The problem to solve is how does a blockchain 'communicate' its high quality (true information known to itself) to potential users, when a competitor blockchain that is actually of low quality (information known to itself, but unobservable) can cheaply but falsely claim that it too is high-quality. The problem is that all blockchains have an incentive to claim that they are high quality, but in fact only some are. This creates a problem for potential users or builders, who need to discern the truth about which blockchains really are high-quality and which are lying.

In Spence's (1973) original model, students and new entrants to the workforce faced the same problems as blockchains - how to communicate to potential employers (cf. users and builders) that they were high quality when every other student was also making the same claim. Spence's argument, which was also discovered in the theory of sexual selection in evolutionary biology (Zahavi 1975), was that those who truly were of high quality (i.e. perhaps smarter and more conscientious) would be able to withstand performing a pointless cost (i.e. had a lower opportunity cost) better than low-quality subjects, and so incurring that cost was a reliable signal of high-quality. High-quality students/blockchains would simply keep increasing that cost until the low-quality students/blockchains dropped out. That point is the separating equilibrium; it is the efficient expenditure on a signal. For Spence, that signal was higher education, which was costly and wasteful, but supplied a credential easily observed by employers. Our argument here is that a large public treasury in a foundation plays the same role as a reliable costly signal. The implicit message is that a strong successful

chain can afford to ‘waste’ vast capital reserves on a large foundation, or, more specifically, that a lessor chain could not afford to sustain such extravagance (i.e. a costly signal), and therefore a small treasury, or no treasury, or a faster burning treasury, is a sign of weakness and vulnerability. The implication is that the optimal size of the foundation treasury is calculated as the separating equilibrium at which the lessor chain cannot carry the burden of the foundation.

Interestingly, a large and valuable foundation that is verifiably on display and available for future dispersal is, in effect, a staked treasury asset: i.e. it is proof-of-stake of proof-of-work. In some cases, a large onchain treasury is also a network security signal, offering a defensive moat against forking. When a software upgrade occurs on a live blockchain, validators sometimes face a choice as to whether to work with the new software or continue to validate the chain with old software. This event is known as a hard fork. Some contentious hard forks result in the creation of two live chains, with a split history at the moment of the software change. The most famous examples are the Ethereum / Ethereum Classic in 2016 and the Bitcoin / Bitcoin Cash split in 2017.

These hard forking events have implications for treasury management. At the event of the hard fork, users who held private keys on the original chain suddenly find themselves holding the keys for accounts or funds on both the original and the new chain. Whoever holds the keys for a treasury now holds treasuries on both chains of the exact same nominal size. If the treasury is a significant proportion of the total tokens on the network, the holder of the treasury keys now has a credible threat to dump one of the chain’s tokens on the market and cause an adverse price shock. The threat of a large treasury is a threat of a hostile actor being one of the biggest token holders on the newly forked network.

**Who pays the costs and receives the benefits of a foundation?**

A foundation treasury is a type of commons, and as such is subject to hazards arising from the tragedy of the commons, i.e. how to stop the treasury from being raided and captured. The basic problem is how to allocate resources from the common pool resource (the treasury) in such a way that the allocation benefits all or most users - i.e. is broadly democratic - but minimises the pitfalls of collective action, of which there are broadly three.

First, the exploitation of the majority by an organised minority (Olson 1960), in which control of key administrative mechanisms - a grants committee, for instance - enables an insider group to extract rents at the cost of outsiders with less.

Second, the exploitation of minority stakeholders by a dominant majority, which arises with unweighted voting that fails to account for strength of preferences or to permit effective side payments or compensation (quadratic voting schemes are designed to mitigate these effects). This is a major problem in any democracy, namely at some point the citizens figure out that they can mount a 51% attack and vote themselves free public goods. This

leads to slow democratic collapse due to exploitation of the minority by the majority (a problem examined by Buchanan and Tullock 1962).[11]

The third is the problem of too much governance and undelegated decisionmaking arising from excessive veto power, or what Buchanan and Yoon (2000) called the problem of the anticommons. Here, the hazard is that few public goods are created because any negative externalities associated with any project that fall on a minority of stakeholders will be sufficient to create a blocking coalition. However, Ostrom (1990) argued that tragedies of the commons tend to be avoided when certain specific governance rules are followed that build on the institutional properties of a community with the ability to communicate, develop local rules, self-monitor and appropriately sanction exploitative behaviour. Buterin (2021) similarly argued that the institutional legitimacy that such governance rules set up in a community furnishes powerful off-chain adaptive security for a blockchain ecosystem.

In the economic theory, the question of who benefits from public goods is trivial: in principle, if they really are public goods, then everyone in the community. But the net beneficiary position is more subtle, because you need to account for the incidence of taxation, i.e. on who the tax burden or its fee equivalent falls, and on other costs that the mechanisms of governance impose. This is the efficiency and equity of premine funding, namely that costs are distributed pro rata over all subsequent token holders. A donation based funding model inevitably pushes costs on to large holders (‘whales’) which runs the corollary risk of tacit collusion or direction by those same parties.

To ask ‘who benefits from a foundation?’ is to ask who benefits from the institutional conditions that a foundation induces, namely by raising the cost of forking there is a lower probability or expectation of forking. So the question is - who benefits from lower probability of forking? The beneficiaries are those who develop idiosyncratic assets or make asset-specific (i.e. chain specific) investments that are at risk of rapid devaluation in the event of an unexpected fork and loss of user base. This is the sense in which lower risk of forking is a kind of insurance that de-risks *asset specific capital investments*.

This situation was analysed in a different context by Williamson (1985) and led to the theory of the institutional efficiency of vertical integration under conditions of asset specificity in investment. The same argument applies here, but with investment in L2 applications vertically integrated into a L1 blockchain. That is, developers and users contributing to aspects of a L2 ecosystem are building assets that have high value on the L1 chain but with a discounted value (possibly zero) on an alternative chain. Their investment problem faces a forking hazard which is difficult to contract through. Developers, builders and users subject to this hazard therefore have an incentive to contribute to, or support in some way, a large fund to minimize that hazard. Obviously, there are free-rider problems here that are exacerbated in any post hoc public finance funding context, and which again points to the superiority of pre-mine (or protocol issuance) funding models.

[11] Also known as Director’s law (Stigler 1970) - this is the observation that public policy will often benefit the middle-class (or median voter) rather than stated intended beneficiaries (e.g. the poor).

**The knowledge problem**

Public goods in a blockchain context also have further problems not generally encountered in nation-state contexts. The first is the bootstrapping problem of launching a blockchain protocol and platform with supporting public goods infrastructure prior to there being a sustaining community to support the creation and delivery of those public goods. This needs to be done in the expectation that if the public goods are supplied the community will come, but needing a source of finance to assure that prospective community that those public goods will eventually arrive. For this reason, mechanisms such as *dominant assurance contracts* (Tabarrok 1998) offer highly promising solutions to this specific bootstrapping problem.

A further aspect of the bootstrapping problem, which is particularly acute in the blockchain context, is that public goods do not start out as provided by a public foundation, but are usually provided by a private organization which must then transition to a public organization, through the process of decentralization. The challenge here is one of credible commitment to continue the decentralization process, which in effect means continually seeking to distribute governance further from its initial point of private centralised origin.

A second broad problem is the knowledge and coordination problem that is due to private provision of novel public goods in the particular aspect of knowing what public goods are needed or desirable, which is a discovery problem of public goods. (Note that such entrepreneurial discovery problems are usually associated with the provision of private goods.) But in the novel context of blockchain ecosystems there are substantial challenges associated with knowing what goods need to be provided and in what order, as distinct from the challenge of how to fund and deliver these goods. The quadratic contribution formulae in gitcoin grants in the ethereum ecosystem, which is a matching pool model using quadratic matching, offers a powerful solution to this problem of funding public goods by exploiting the assumption that if a lot of different people all propose the same good than it is likely to be a better public good than one that only a few want. Gitcoin grants are thus incentive compatible with public matching of private funding to identify high-quality public goods (Pasquini 2020).

A third broad problem is the challenge of this process of supply of public goods in the context of an O-Ring type production technology (Kremer 1993), such that there are many parts to the public goods infrastructure, occurring across multiple simultaneous nodes or sites and the need to ensure that the overall complementary structure of public goods individually provided (i.e. the various components of infrastructure) assembles into a functional system. The challenge is to do so without centralised decision-making (or a decentralised price mechanism) to coordinate all the individual plans to enable them to ensure they mesh properly and to minimize inefficient duplication of effort to ensure that essential tasks are done and critical infrastructure or services are provided at all.[12]

[12] Also known as the 'Richardson problem' - named by Peter Earl, referencing Richardson (1960).

# 5 Conclusion

Almost all Layer 1 blockchain projects have developed supporting foundations. Some of these were conceived and launched simultaneously with the mainnet protocol, and as others have developed subsequently. Many are extremely large, with substantial treasury assets (usually held as a native token). Almost all are designed as non-for-profit foundations, governed by a professional board, and which perform a range of tasks broadly associated with providing public goods and infrastructure support and services to the blockchain ecosystem. Most compensate teams of developers maintaining and developing the codebase, as well as supporting broader R&D projects that benefit the ecosystem (e.g. through grants programs). Some undertake marketing, education, lobbying and public relations.

From this perspective crypto foundations look a lot like governments: they play the same role of providing public goods and economic infrastructure to a blockchain ecosystem.[13] The provision of public goods in a nation state economy is the task of a government, drawing on its ability to raise taxes and put those public finances to use supplying economic infrastructure, which in the physical world means providing transport, trade and communications infrastructure, as well as institutional infrastructure such as courts, money, and administration. Governments also provide security of property and defence against external threats. In this view, a blockchain foundation plays an analogous role, providing essential economic infrastructure, including economic security, to a crypto-economy. A crypto foundation, in this model, is a private government providing club goods.

However, we have argued that a blockchain foundation also performs another crucial function: namely that of raising exit costs, particularly those associated with forking, which by mutually reinforcing the expected costs of exit actually incentivises long term investment on the platform. A foundation, in this view, is a costly moat that facilitates economic development by aligning expectations about the likelihood that other parties in the ecosystem will stick around. This is because the existence of the foundation creates an opportunity cost for them leaving. The larger the foundation, the higher the opportunity cost.

In the theory proposed here, a large, slow-moving endowment that is used as a pool to fund public goods (including developers, research, code maintenance, etc.) is actually also functioning as forking insurance. The foundation is precisely that which you can't take with you if you fork, so the existence of a foundation raises the cost to forking (in proportion to the size of the foundation). This in turn furnishes stability in the ecosystem due to rational expectations of other users and stakeholder's likelihood of exit being mutually revised downwards.

Two important implications of our theory is that there will be an optimal size to the treasury fund, and that friction in spending or drawing it down is actually a feature. These insights also implies that if you want a lot of public goods on a chain, and especially if you want them early - i.e. that there is a need for early and significant draw-down of the fund -

[13] Note that economic infrastructure includes both physical infrastructure (roads, ports, communications networks, physical security, etc) and administrative infrastructure (registries for identity and property, laws and regulation, democratic governance, etc). See Frischmann (2012) for a general theory of common pool infrastructure.

then that will work against the role of the fund in providing forking insurance and the expectation of persistence. So, if that function is required, then a different mechanism to cover large-scale early spending on public goods, other than the fund, will be needed. A large public goods fund is an effective mechanism to create an implicit threat to exit, which is then attractive to those who seek to join and commit asset specific investments that are at hazard of forking. A foundation, in this view, is both castle and moat.

## References


Alchian, A. (1950) 'Uncertainty, evolution, and economic theory' *Journal of Political Economy*, 58(3): 211-221.

Benkler, Y. (2006) *The Wealth of Networks*. Yale University Press: New Haven.

Berg, C. (2020) 'Rent seeking in blockchain governance', RMIT BIH working paper.

Bergstrom, T., Blume, L., Varian, H. (1986) 'On the private provision of public goods' *Journal of Public Economics*, 29(1): 25-49.

Buchanan, J., Tullock, G. (1960) *The Calculus of Consent.* University of Michigin Press: Ann Arbor.

Buchanan, J. (1965). An economic theory of clubs. *Economica*, 32(125): 1-14

Buchanan, J., Yoon, Y. (2000) 'Symmetric tragedies: Commons and anticommons' *Journal of Law and Economics*, 43

Buterin, V. (2021) 'The most important scarce resource is legitimacy' https://vitalik.ca/general/2021/03/23/legitimacy.html

Davidson, S. (2021) 'Governance of blockchain foundations.' RMIT BIH working paper.

Eghbal, N. (2020). *Working in Public: The Making and Maintenance of Open Source Software*. Stripe Press.

Frischmann, B. (2012). *Infrastructure: The social value of shared resources*. Oxford University Press.

Frischmann, B. Maddison, M., Strandberg, K. (eds) (2014) *Governing Knowledge Commons*. Oxford University Press: Oxford.

Hansmann, H. (1996) *The Ownership of Enterprise*. The Belknap Press. Cambridge, MA.

Kremer, M. (1993) 'The O-ring theory of economic development' *Quarterly Journal of Economics*, 108(3): 551-575.

Lerner, J., and J. Tirole (2002), 'Some Simple Economics of Open Source', *Journal of Industrial Economics*, 52: 197–234.

Lerner, J., and J. Tirole (2005), 'The Economics of Technology Sharing: Open Source and Beyond', *Journal of Economic Perspectives*, **19**(2): 99–120.

Nair, M., Sutter, D. (2018) 'The blockchain and increasing cooperative efficacy' *The Independent Review*, 22(4): 529-550.

Olson, M. (1960) *The Calculus of Consent*. Harvard University Press: Cambridge MA.

Ostrom, E. (1990) *Governing the Commons*. Cambridge University Press: Cambridge.

Ostrom, E., Hess, C. (2003) ‘Ideas Artifacts and Facilities: Information as a Common-Pool Resource’, *Law & Contemporary Problems*, 66(1/2): 111–145

Pasquini, R. (2020) ‘A Note on Quadratic Funding under Constrained Matching Funds’ *arXiv preprint arXiv:2010.01193*

Potts, J. (2019) *Innovation Commons*. Oxford University Press: Oxford.

Raymond, E. (1999) *The Cathedral and the Bazaar*. O'Reilly Media: Sestapol, CA.

Richardson, G. (1960) *Information and Investment: A Study in the Working of the Competitive Economy*, Oxford University Press: Oxford.

Samuelson, P. (1954) ‘The pure theory of public expenditure,’ *Review of Economics and Statistics*, 36(4): 387–389

Spence, M. (1973) Job market signaling’ *Quarterly Journal of Economics*. **87** (3): 355–374

Stigler, G. (1970) ‘Director’s law of public income distribution’ *Journal of Law and Economics.* 13(1)

Tabarrok, A. (1998) ‘The private provision of public goods via dominant assurance contracts’ *Public Choice* 96: 345–362.

Tiebout, C. (1956) ‘A pure theory of local expenditures’, *Journal of Political Economy* 64 (5): 416–424.

Williamson, O. (1985) T*he Economic Institutions of Capitalism: Firms, Markets and Hierarchies*. Free Press: New York.

Williams, M., Hall, J. (2015), ‘Hackerspaces: A Case Study in the Creation and Management of a Common Pool Resource’, *Journal of Institutional Economics*, 11(04): 769–781.

Zahavi, A. (1975) ‘Mate selection: a selection for a handicap’ *Journal of Theoretical Biology*, 53(1): 205-214.