Market Design for a Blockchain-Based Financial System*

[Extended Abstract]

Christian Catalini
Calibra, Inc.

Ravi Jagadeesan
Harvard University

Scott Duke Kominers
Harvard University

June 18, 2019

Abstract

We develop a theory of long-run equilibrium in blockchain-based financial systems. Our theory elucidates the key market design features that separate proof of work and proof of stake approaches in the long run. Under proof of work, wasteful computation is used to secure the system, and users' utility in equilibrium is determined by the threat of a fork. Under proof of stake, by contrast, users' utility in equilibrium is generally above the fork threat level because custodians can use relational contracts to incentivize a higher quality of service. Relational contracts under proof of stake rely only on local institutions—but combining them with cryptography can create a platform for formal global contracts.

*This research was supported in part by Calibra, Inc., a subsidiary of Facebook, Inc.. Catalini is Head Economist for Calibra, Inc., and Kominers is an advisor for Calibra, Inc.. While working on this research, Jagadeesan was a National Science Foundation Graduate Research Fellow under Grant No. DGE-1745303.
Email addresses: catalini@calibra.com, rjagadeesan@hbs.edu, and kominers@fas.harvard.edu.

Traditional financial systems maintain trust through formal and relational contracts supported by enforcement mechanisms such as courts. The resulting economies of scale drive a natural tendency towards concentration. While concentration increases efficiency, it also results in higher transaction fees, barriers to entry, and a potentially suboptimal level of innovation. By assigning control over financial infrastructure and its governance to trusted intermediaries, concentration also reduces the resilience of a financial system to failure and interference by third parties.

Over the last decade, blockchain technology has emerged as a way of coordinating economic activity—without assigning as much control to trusted intermediaries—by using cryptography to create a transaction layer that can act as a true public utility. Yet while cryptography and technology constrain the theoretical maximum performance of blockchain systems, the levels of efficiency, security, and decentralization that are actually achieved depend crucially on the *market design* of the ecosystem.

The blockchain market design pioneered by Bitcoin (Nakamoto, 2008) relies on wasteful computation—or *proof of work*—to protect the network from attempts to rewrite the shared ledger of transactions. Under proof of work, participants' impacts on the flow and history of transactions are linked to their computational powers, ensuring that the agents (called *miners*) who operate and secure the system cannot gain disproportionate influence via "sybil attacks." To perform the wasteful computations that are required under proof of work, miners must invest in specialized infrastructure; these investments add security because they make it difficult to build up enough computational power to subvert the network. But wasteful computation is, quite literally, wasteful. To eliminate the need for it, alternative market designs are being developed in which participants' influence is linked to their demonstrated holdings of currency or other stakes in the system—i.e., their ability to provide a *proof of stake*.

Despite the rapid expansion of blockchain technology—and a growing body of economic

analysis of the topic[1]—there has so far been limited research on which blockchain-based market designs might be most successful at scale. As a step in this direction, we develop a theory of long-run equilibrium in blockchain-based financial systems. Our theory elucidates the key market design features that separate proof of work and proof of stake approaches in the long run.

In our model, there are *nodes* that process and verify transactions,[2] as well as *custodians*, which hold users' assets. Relational contracts between nodes and custodians—as well as wasteful computation by the nodes—can secure the system and hence reduce the risk of catastrophic failure. However, concentration in the node market increases the risk of failure (e.g., by lowering the cost of a targeted attack on the nodes). In addition to securing the system, nodes determine the rate at which transactions are executed (through, e.g., the "block size") and the overall quality of service users experience. If the throughput of transactions or the quality of service is too low, or if the node market becomes too concentrated, then custodians can attempt to fork the system. If a fork attempt succeeds, then existing nodes' investments in specialized computational infrastructure are wiped out and the node market becomes temporarily disperse.[3]

Under proof of work, the influence of a node over transactions is a function of that node's relative computational power. Furthermore, relational contracts between nodes and custodians are not enforceable because it is not possible to selectively exclude misbehaving (or *byzantine*) nodes from the system. Therefore, the only constraint on nodes' actions is through the ability of custodians and/or users to coordinate around a fork. In long-run

[1]See, for example, the work of Böhme, Christin, Edelman, and Moore (2015); Athey, Parashkevov, Sarukkai, and Xia (2016); Catalini and Gans (2016, 2018); Halaburda and Sarvary (2016); Raskin and Yermack (2016); Athey, Catalini, and Tucker (2017); Catalini and Tucker (2017); Huberman, Leshno, and Moallemi (2017); Abadi and Brunnermeier (2018); Budish (2018); Sockin and Xiong (2018); Tucker and Catalini (2018); Biais, Bisiere, Bouvard, and Casamatta (2019).

[2]Under proof of work, nodes in our model represent miners. We use a broader term to encapsulate transaction-clearing agents under proof of stake as well.

[3]In the model, we focus on hard forks that force nodes to make new technological investments by rendering existing specialized infrastructure incompatible with the protocol—e.g., by changing the type of wasteful computation that nodes must perform. If nodes have not developed infrastructure for the new computational tasks in advance, then a hard fork will lead to temporary dispersion in the node market.

equilibrium, the threat of a fork ensures a baseline level of utility for the users. In particular, there is an upper bound on the possible risk of catastrophic failure the system will tolerate in equilibrium; this bound implies a baseline level of dispersion in the node market will be sustained. That said, as nodes can save costs by reducing quality of service, the threat of a fork will bind in equilibrium, making the users' utility exactly equal to the baseline level. Moreover, if coordinating on a fork is difficult at scale, then the baseline level of utility will be low—making users' utility under proof of work low in equilibrium.

Under proof of stake, the influence of a node over transactions is a function of the relative stake that the node controls either directly or through delegation. As custodians can freely change which nodes they delegate their stakes to, relational contracts between custodians and nodes can play a role in the equilibrium. In the extreme case in which relational contracts are perfect, wasteful computation has no marginal benefit. In contrast, with weaker relational contracts, some degree of wasteful computation can improve the security of the system. Thus, the extent to which gains in efficiency are possible relative to proof of work depend on the quality of the institutional environment—and hence vary by jurisdiction. However, relational contracts are only needed to discipline the behaviors of the nodes to whom custodians delegate stake. As a result, strong local institutions supporting delegation can be sufficient to sustain a global system under proof of stake. Cryptography thus complements local institutions by leveraging them to provide a platform for formal global contracts.

In addition to providing potential efficiency gains relative to proof of work, proof of stake also leads to improvements in incentives and market structure. Specifically, the ability of custodians to choose a delegate allows users to discipline the observable dimensions of nodes' behavior without having to coordinate on a fork, while relational contracts give users some ability to discipline the unobservable dimensions. In particular, in equilibrium under proof of stake, the threat of forking may not be the binding constraint on nodes' actions, meaning that users can obtain utility above the baseline level. As a result, users' utility in equilibrium is determined by technology and the costs of securing the network, instead of by

the threat of a fork. This feature is particularly relevant at scale, when coordination between custodians/users might be difficult. Similarly, equilibrium concentration under proof of stake is determined by a trade-off between efficiency and security, instead of by a baseline level of dispersion as under proof of work.

The use of relational contracts may also enable faster coordination around governance decisions. At the same time, however, the use of relational contracts under proof of stake could make the system more vulnerable to interference by third parties. Indeed, nodes are substitutable under proof of work by construction, whereas nodes' identities and off-network reputations can play a role in sustaining equilibrium under proof of stake. Therefore, there is a design trade-off between the use of relational contracts to improve efficiency and incentives, and the degree to which the system is vulnerable to interference. Moreover, the presence of relational contracts imparts custodians with a more prominent role in the ecosystem. If trust in custodians becomes an important issue, then the market for custody might become concentrated; this concentration might be undesirable *per se*, and it might lead to another vector for third party interference.

Overall, our analysis suggests when proof of work designs and proof of stake designs might each be appropriate. With weak relational contracts or substantial concerns about outside interference, proof of work designs may be preferable. In contrast, when some regions have local institutions that are reliable enough to make delegation feasible, proof of stake designs can lead to efficiency gains and improvements in governance. If successful, proof of stake designs would then use cryptography to leverage these local institutions to create a platform for formal global contracts—providing spillover benefits to regions with weaker local institutions.

References

Abadi, J., and M. Brunnermeier (2018): "Blockchain Economics," *Working Paper No. 25407, National Bureau of Economic Research*.

Athey, S., C. Catalini, and C. Tucker (2017): "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *Working Paper No. 23488, National Bureau of Economic Research*.

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia (2016): "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence," *SSRN Working Paper No. 2826674*.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019): "The Blockchain Folk Theorem," *Review of Financial Studies*, 32(5), 1662–1715.

Böhme, R., N. Christin, B. Edelman, and T. Moore (2015): "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives*, 29(2), 213–238.

Budish, E. (2018): "The Economic Limits of Bitcoin and the Blockchain," *Working Paper No. 24717, National Bureau of Economic Research*.

Catalini, C., and J. S. Gans (2016): "Some Simple Economics of the Blockchain," *Working Paper No. 22952, National Bureau of Economic Research*.

——— (2018): "Initial Coin Offerings and the Value of Crypto Tokens," *Working Paper No. 24418, National Bureau of Economic Research*.

Catalini, C., and C. Tucker (2017): "When Early Adopters Don't Adopt," *Science*, 357(6347), 135–136.

Halaburda, H., and M. Sarvary (2016): *Beyond Bitcoin: The Economics of Digital Currencies*. Springer.

Huberman, G., J. Leshno, and C. C. Moallemi (2017): "Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System," *SSRN Working Paper No. 3032375*.

Nakamoto, S. (2008): "Bitcoin: A Peer-to-Peer Electronic Cash System," *White Paper*.

Raskin, M., and D. Yermack (2016): "Digital Currencies, Decentralized Ledgers, and the Future of Central Banking," *Working Paper No. 22238, National Bureau of Economic Research*.

Sockin, M., and W. Xiong (2018): "A Model of Cryptocurrencies," *Working Paper, Princeton University*.

Tucker, C., and C. Catalini (2018): "What Blockchain Can't Do," *Harvard Business Review*.