Antitrust and Costless Verification: An Optimistic and a Pessimistic View of the Implications of Blockchain Technology

Christian Catalini and Catherine Tucker[*]

June 19, 2018

Abstract

Blockchain technology allows a network of individuals, institutions or devices to coordinate economic activity on a global scale ('internet-level consensus') without assigning the same degree of control to the intermediary operating and facilitating transactions in the marketplace. This allows for the creation of new types of decentralized digital platforms where the benefits of network effects are separated from the traditional costs they entail in terms of market power. We discuss both the opportunities and challenges the technology involves from an antitrust perspective, and in particular how it can be used to facilitate the creation of extremely efficient and competitive digital markets, as well as to facilitate collusion and make antitrust enforcement more difficult.

[*] Christian Catalini: MIT Sloan School of Management, MIT Cryptoeconomics Lab and NBER (catalini@mit.edu). Catherine Tucker: MIT Sloan School of Management, MIT Cryptoeconomics Lab and NBER (cetucker@mit.edu).

1 Introduction

Transactions between individuals or organizations typically involve trust that transactions will be executed as planned. Or, if trust is not enough, they may rely on third parties to enforce contractual arrangements and verify that exchanges of goods or services actually went through as promised. Blockchain technology, by allowing economic agents to verify transactions and their attributes without the same need for trust or third-party verification, fundamentally changes how marketplaces operate. This is particularly relevant for digital marketplaces. Blockchain technology lowers the cost of verifying digital information but does not lower the cost of verifying offline information.[1]

At a high level, blockchain technology allows a network of economic agents (individuals, firms, devices etc) to agree, at regular intervals, about the true state of some jointly curated, shared and maintained data. This shared data can represent ownership or balances in a cryptocurrency (a 'distributed ledger', as in Bitcoin or Ethereum), but also in other types of digital assets such as financial assets, equity or property rights on digital resources such as file storage, digital content, and information. Any update or change to the shared data is secured through a clever mix of cryptography and economic incentives, and can be extended through the use of smart contracts, which are software contracts that define which transformations should be applied to the data in response to different types of events. Since no intermediary is needed to perform the custody or an exchange of assets recorded on a blockchain, for the first time in history the technology allows for value and digital assets to be reliably transferred between distant parties without any external institution or organization.

On the face of it, when described in this manner, it can be difficult to see how blockchain technology may influence antitrust, except for potentially reducing its scope. After all,

[1] In other work we discuss this constraint in detail. For example, imagine a digital newborn baby tracking platform - though this is useful for ensuring the integrity of the digital data tracking baby movements - it does not verify that the actual baby itself is tagged with the right identifier.

blockchain technology seems to reduce costs of the type that can otherwise lead to centralization and entrenched market power in digital platforms. This article will argue, however, that if blockchain technology develops in the way that its evangelists expect, it will pose an unparalleled set of novel challenges for antitrust, which will be greater and less easily solved than even the problems posed by the rise of large digital platforms which have absorbed much scholarly attention over the last decade.[2]

In particular, we emphasize two major points. First, there is considerable reason to think that the decentralized nature of some blockchain implementations may be beneficial for antitrust concerns and reduce the need for antitrust enforcement. We term this the 'optimistic view' of the technology. Second, there is also reason to believe that the technology may pose practical challenges for antitrust enforcement. We emphasize that antitrust law is set up on the premise that there is a clearly demarcated firm (or set of firms) that may try and seek market power. The decentralized nature of the technology means that identifying an entity to prosecute or hold responsible for any degree of market power (or its abuse) is impossible, and that collusion and price setting between competitors may be harder to detect.

1.1 An Economic Perspective on Blockchain Technology

Before we embark on the main thrust of our argument, it is useful to expand on how blockchain technology takes advantage of cryptography and incentives to replace trust and third-party verification. From an economics perspective, an implementation of blockchain technology has two key characteristics as a technological solution:

1. **A set of shared data** – in the case of the well-developed use-case of cryptocurrencies,

[2] See, for example, https://www.wired.com/2017/06/ntitrust-watchdogs-eye-big-techs-monopoly-data/ for the new types of issues such as the treatment of two-sided markets, network effects, digital privacy and data by antitrust authorities that the rise of digital platforms has brought. For a scholarly overview, see Evans and Schmalensee (2013).

these are digital ledger entries that form, over time, an immutable audit trail of all past transactions and ownership records in the underlying digital asset. As assets, such as bitcoin, are exchanged between users, the shared data is updated to reflect the corresponding changes in ownership and allow participants to verify, without relying on an intermediary, that the transaction has successfully taken place.

2. **An incentive system** ('consensus rules') – designed to ensure that the shared data can only be updated in a way that reflects the truth. Incentives are needed to protect the shared data from being altered by an adversary or bad actor, and to ensure that transactions or assets cannot be forged or modified *ex post*. For example, in implementations that rely on proof-of-work ('mining'), an economic cost is introduced to make it prohibitively expensive to rewrite history and subvert the consensus about the true state of the shared data once it is formed.

The shared data is probably most easily imagined as the information recorded in a large, append-only log of transactions where each entry is time-stamped and cryptographically linked to previous entries. Such cryptographic link forms, as time passes, an immutable chain between subsequent blocks of transactions (hence, a 'blockchain'). Full network participants in a blockchain protocol, who are sometimes referred to as 'full nodes', keep a copy of the entire shared data and help broadcast new transactions to the rest of the network as they arrive. In systems that rely on 'mining' to secure the shared data, a special set of mining nodes also performs wasteful computations - a sunk cost - to make it extremely expensive for an attacker to alter the history of the shared data and revert a valid transaction. In a blockchain protocol, the immutability of the records is therefore the result not simply of cryptography, but of the economic incentives targeted at forming and maintaining an honest 'consensus' about what the shared data should represent at any moment in time. Participants in a blockchain protocol have an incentive to collaborate to prevent 'greedy attackers' from defrauding the system (Nakamoto, 2008).

From an antitrust perspective, therefore, the most crucial component of blockchain technology to understand is the type of incentive system put in place to protect the shared data. As one might expect, a key element is who can participate in the broadcasting of new transactions, maintenance of the shared data and formation of consensus:

1. **Permissionless blockchains**[3] such as Bitcoin and Ethereum allow anyone to participate as long as they follow the rules of the protocol. Whereas participation may require dedicating resources to the network through computing power or storage, the network is completely indifferent as to who provides such resources. This means that barriers to entry and participation are typically extremely low. Furthermore, updating the shared data is a process that requires consensus among network participants (e.g. a majority of the nodes supporting the change), hence no single participant can change the shared data through a unilateral move.

2. **Permissioned blockchains** (sometimes also referred to as private blockchains) instead offer greater control to some of the participants, and may restrict the ability to write or read part of the data to a subset of trusted nodes such as an organization that is part of a consortium. In cases where trusted nodes have full control over the process that updates and maintains the shared data, permissioned blockchains are very similar to the distributed databases companies have been using for decades, and provide little advantage over pre-existing solutions (except perhaps for simpler settlement and reconciliation of records across different organizations).

[3] Sometimes this distinction is presented as 'private' versus 'public' blockchains. We use the terms 'permissionless' versus 'permissioned', as they are more precise.

2 An Optimistic View of What Blockchain Means for the Future of Antitrust

We start by re-emphasizing that in theory, blockchain technology should reduce market power in digital platforms. To understand this, it is useful to contrast the types of platforms that can be created using blockchain technology with traditional digital platforms. Typically, there are three reasons why digital platforms which bring together multiple groups of users to interact or transact over a single technology infrastructure (such as Google, Facebook, Amazon etc.) have attracted attention from antitrust authorities. Though the economics behind whether such concerns are warranted is unclear (Evans and Schmalensee, 2013), and these concerns are not new,[4] it is useful to see how blockchain alleviates some of these concerns.

First, a key concern expressed about digital platforms is that the scale of their information collection activities may lead to increased market power, making it extremely difficult for new entrants to compete against progressively more entrenched incumbents. As pointed out by Stiglitz (2002), if one firm alone is trusted to verify transactions or acts as the key intermediary in a large number of transactions in a marketplace, this will lead to an informational advantage over competitors as well as buyers and sellers. By having a comprehensive picture of most interactions in a marketplace, a digital platform can exploit information asymmetry between the different sides of the market to its own advantage.[5] For example Amazon, by having access to both fine-grained customer and seller performance data, can use this to decide which products to integrate within its direct offerings versus not, ultimately competing with some of the sellers that drove traffic to its platform in the first place.[6] In

[4] See for example US Airways Inc v. Sabre Holdings Corp et al, U.S. District Court, Southern District of New York, No. 11-cv-2725. which contemplated these issues in the context of airlines reservations.

[5] Other authors, such as Lambrecht and Tucker (2015), have argued, however, that data by itself is unlikely to confer competitive advantage, given that it is costless to replicate and non-rival in consumption.

[6] See also Bajari et al. (2018) for empirical evidence on this point. This paper suggests there are returns

such a context, a system based on blockchain technology where all entities have equal access to information about transactions, and no one firm owns the information involved in transactions, could reduce the potential for market power that comes from instances where information is difficult to acquire, not easy to duplicate, and constitutes a friction between market participants.

Second, another set of concerns expressed about digital platforms is that they naturally give rise to network effects. Network effects occur when a digital platform delivers more utility to a user as additional users join the platform too (direct network effects), or as more applications are developed on top of that platform (indirect network effects). This can lead to platforms that are larger in scale to be more attractive than smaller ones (see Tucker (2018) for a discussion of how digital platforms today are less vulnerable to this critique than earlier platforms). In theory, blockchain technology can be used to overcome the coordination challenges that otherwise lead network effects to be a source of market power (Catalini and Gans, 2016), as it allows platform architects to design digital ecosystems where the benefits from adoption and growth are shared among different stakeholders such as users, developers of complementary applications, and providers of key resources. An example of this would be a blockchain platform that uses a crypto token – that is a native digital asset that functions as the exclusive medium of exchange for transactions on the platform – to incentivize early adopters[7] or early developers to invest time and resources on the platform. Whereas such platform-specific tokens are worthless when the platform is small and processes a small number of transactions, they appreciate in value as the platform scales, automatically rewarding early contributors for taking risk and supporting the development of the platform when its success was uncertain (Catalini and Gans, 2018). This allows

to data for forecasting demand for a particular product over time, but few gains from predicting performance across product categories from big data.

[7] Early adopters can play a key role in accelerating or slowing down the diffusion of new blockchain-based platforms; see Catalini and Tucker (2017).

blockchain-based platforms to solve the coordination problems that make it usually difficult for users or developers to abandon dominant platforms, decoupling the benefits from network effects (and from being able to rely on a shared standard and infrastructure) from the costs of market power.

Third, related to network effects is the issue of how easy it is for users or suppliers to multihome and simultaneously use competing platforms. Switching costs reinforce market power by making it harder for users to seamlessly move between platforms, for example to take advantage of better prices or offers. A typical example of a switching cost would be that if I have a complete library of digital music in a proprietary Apple format, I would find it costly to switch to buying digital music from another platform as it would be inconvenient to have my music stored in different places. Switching costs have been at the center of multiple antitrust cases, including the Microsoft browser case where the DOJ argued that the company was leveraging its market share and monopoly power in the operating system space to extend its influence in the emerging internet one. As operating systems have become less of a friction for users because of a shift to web and mobile applications, the trend has been to make multihoming easier - for example, drivers and customers are able to seamlessly alternate between Uber and Lyft rides by simply switching between apps on their phones. Echoing this, blockchain implementations are increasingly focused on reducing switching costs for users, and allowing applications built on top of different protocols to exchange data or even to directly transact with each other. This is facilitated by the fact that most permissionless platforms are built as open source code and therefore allow other applications and platforms to interface with their network as long as they comply with the requirements of their protocol. Moreover, many platforms have a native token that not only facilitates exchanges on the platform, but also makes it extremely easy to convert assets between different ecosystems: Similar to financial markets, where exchanges allow users to trade one type of financial asset or currency for another, cryptocurrency exchanges allow users to move in and out of different tokens with minimal frictions. The exchange and trading process is likely to improve and become more automated as decentralized exchanges (which are exchanges that do not rely on an intermediary to match buyers and sellers) further diffuse. In the case of cryptocurrency, most digital wallets already support a number of different crypto tokens, allowing users to seamlessly move between digital assets stored on different blockchains. Such technological applications make it easier for a user who wishes to use multiple implementations to do so; indeed, the process becomes virtually costless.

Last, it is worth mentioning the technological peculiarities of ‘forking,’ which increase the competitive pressure on any blockchain-based platform and the team managing its evolution. Since the codebase of permissionless blockchain protocols is typically open source, if a group of users or developers is unhappy with the team maintaining the code or with the rules through which the protocol forms consensus over time and allocates rewards to contributors, it can fork the codebase together with the entire history of transactions and start a separate, backwards compatible blockchain. This has happened multiple times in the history of the major cryptocurrencies, Bitcoin and Ethereum, and has been motivated both by attempts to change the incentive system (for example to reduce the market power of specific participants, such as miners), as well as for addressing disagreement about technical and governance decisions. The ability to fork a blockchain in this manner means that in theory any permissionless blockchain faces constant and real competition from being forked if it is judged to not be optimizing the welfare of its different participants. Moreover, if such a fork offers better governance or is more competitive, it will quickly gather users and developers since switching costs are extremely low.

3 A Pessimistic View of What Blockchain Means for the Future of Antitrust

Given this optimism about the effects of blockchain technology on the need for antitrust enforcement, it may be surprising to think that blockchain may also pose huge difficulties for antitrust authorities should there ever need to be enforcement. In the same way the decentralized nature of blockchain technology allows for network effects to emerge without assigning market power to a platform operator, the absence of a central entity could constitute a challenge for antitrust. Intellectually and practically, antitrust enforcement is designed to tackle instances where market power has been centralized, and consequently has not been set up for cases where there are explicit rules designed to ensure decentralization.

Typically antitrust authorities try to stop entrenched firms from using their market power to harm consumer welfare; in parallel they also maintain guidelines for horizontal and vertical mergers, analyze proposed mergers and block actions that might allow merged firms to use their resulting market power to hurt consumer welfare. In both of these cases, there is a clear notion of a firm (or perhaps, in the case of a cartel, a consortium of firms) which can be the focus of an investigation, and which will be a target for potential fines and prosecution. Blockchain technology is different because it removes the need for a firm to manage the transactions that occur on a digital platform. Indeed, the entire premise of a permissionless blockchain-based platform is that it has merit because it is completely decentralized and does not need a single entity to sponsor it or any actual firm or third-party to support its operations. Whereas the market is nascent and currently no cryptocurrency or blockchain project has reached any meaningful market power, at scale some of the projects will have enough market share to influence prices and consumer welfare. If the suppliers of resources (e.g. miners in an ecosystem like Bitcoin, data storage providers in a decentralized storage network like Filecoin or Sia) use their control over key inputs to shape competition on a decentralized marketplace in their favor, it will be difficult for antitrust to intervene, as many of these suppliers could be small, hard to identify and geographically dispersed. Similar tensions have already materialized within the Bitcoin ecosystem between miners and the developers of consumer-facing applications (e.g. payments, digital wallets etc), since the two sides have conflicting incentives regarding how to scale the Bitcoin network to support more transactions per second.[8]

It may be tempting therefore for antitrust authorities to think that any enforcement actions should be directed at the initial architects of a blockchain platform. However, given the fact that the most successful implementation of blockchain technology so far - Bitcoin - was set up by an individual (or group of individuals) who has managed to remain anonymous for a decade despite having access to holdings of the cryptocurrency worth billions of dollars, there are reasons to doubt that the identification of the initial architects will always be practical. Even in cases where it is possible to identify the initial architects, it is not clear it would be reasonable to target any enforcement action at them, since if the system is truly decentralized they would not have the power, as individuals, to alter or influence its evolution. All they could do is advocate for specific changes to be implemented, possibly by supporting a fork of the network. Indeed, the only way to change the rules of a decentralized platform at scale would be through a 'network vote', which would require the majority of participants to support the new direction.

Additionally, the question of 'intent' is far more nebulous within a decentralized system, meaning that antitrust authorities' reliance on internal documents within a firm to establish intent is unlikely to be implementable in a cost-effective way for all actors participating in a

[8] Congestion on the network increases the fees users have to pay for each transaction and therefore the revenues miners derive from securing and validating the Bitcoin ledger. This constitutes an obstacle for broader adoption by consumers and for use cases that require low fees (e.g. retail payments, micropayments), and creates tension between the miners that do not want to support changes to the protocol that would increase capacity, and application developers building products in those areas that need such capacity to deliver a competitive user experience in the first place.

decentralized blockchain (many of which may be located in different jurisdictions and may be difficult to identify).

We end by noting two more traditional ways that deviations from the premise of a permissionless blockchain could lead to more traditional market power concerns.

Permissioned blockchains have much in common with traditional databases. The major difference is that, unlike in a database controlled by a single entity, a blockchain-based ledger may have accurate historical records of all changes made to a piece of information replicated across multiple entities. For example, a financial blockchain could span multiple banks or financial institutions operating in the same market. In theory, of course, better transaction record-keeping may make electronic discovery easier for antitrust (and other) authorities. However, the current state of the rules surrounding electronic discovery and the format in which such data is delivered in the legal system is one of disarray, often making it expensive to extract critical information in a cost effective manner. The effect of blockchain on e-discovery is therefore not clear and may involve transition costs (Miller and Tucker, 2012), and in the case of encrypted data could lead to situations where antitrust authorities have no way of recovering the original information, for example if the encryption keys have been destroyed.

It is also important to highlight that permissioned blockchains are not necessarily immutable, and key participants could technically collude to rewrite the log of transactions before discovery takes place. Furthermore, under the guise of the need to protect confidential information or privacy, participants in a permissioned system could tightly control which participants receive access to different pieces of information, leading to entrenchment of market power.

The risk of collusion is also present when industry-based consortia are formed to develop a shared blockchain solution. 40 consortia have been formed over the past six months[9],

[9] See https://www2.deloitte.com/insights/us/en/focus/signals-for-strategists/

the majority of which are focused on financial services. As ever, when competing firms work together, there is the potential that this repeated contact could facilitate collusion. This possibility was discussed in detail by Cong and He (2018), who argue that a potential solution is to regulate for separation of consensus record-keepers from users. Furthermore, a distributed ledger could be used in theory to allow for better monitoring of collusive price arrangements, as participants could design it in a way that allows them to deanonymize the transactions of competitors or at least observe aggregate transaction patterns. This could be enhanced by the use of smart contracts and artificial intelligence to automatically respond to changes in the marketplace or actions by participants, further obfuscating collusive actions and facilitating the implementation of price or quantity setting arrangements.

emergence-of-blockchain-consortia.html

References

Bajari, P., V. Chernozhukov, A. Hortaçsu, and J. Suzuki (2018). The impact of big data on firm performance: An empirical investigation. Technical report, National Bureau of Economic Research.

Catalini, C. and J. S. Gans (2016). Some simple economics of the blockchain. *SSRN Working Paper No. 2874598, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598*.

Catalini, C. and J. S. Gans (2018). Initial coin offerings and the value of crypto tokens. *SSRN Working Paper No. 23137213, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213*.

Catalini, C. and C. Tucker (2017, July). When early adopters don't adopt. *Science 357*(6347), 135–136. Science.

Cong, L. W. and Z. He (2018). Blockchain disruption and smart contracts. Technical report, National Bureau of Economic Research.

Evans, D. S. and R. Schmalensee (2013, February). The antitrust analysis of multi-sided platform businesses. Working Paper 18783, National Bureau of Economic Research.

Lambrecht, A. and C. E. Tucker (2015). Can big data protect a firm from competition?

Miller, A. R. and C. E. Tucker (2012). Electronic discovery and the adoption of information technology. *The Journal of Law, Economics, and Organization 30*(2), 217–243.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*.

Stiglitz, J. E. (2002). Information and the change in the paradigm in economics. *American Economic Review 92*(3), 460–501.

Tucker, C. (2018). What have we learned in the last decade? network effects and market power. *Antitrust Journal*.