

## MIT Open Access Articles

*Some simple economics of the blockchain*

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

**Citation:** Catalini, Christian and Joshua S. Gans. "Some simple economics of the blockchain." Communications of the ACM 63, 7 (June 2020): [dx.doi.org/10.1145/3359552](https://doi.org/10.1145/3359552). © 2020 Owner/Author

**As Published:** <http://dx.doi.org/10.1145/3359552>

**Publisher:** Association for Computing Machinery (ACM)

**Persistent URL:** <https://hdl.handle.net/1721.1/130500.2>

**Version:** Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

**Terms of Use:** Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.



## **Blockchain technology can shape innovation and competition in digital platforms, but under what conditions?**

BY CHRISTIAN CATALINI AND JOSHUA S. GANS

# Some Simple Economics of the Blockchain

IN OCTOBER 2008, a few weeks after the Emergency Economic Stabilization Act rescued the U.S. financial system from collapse, Satoshi Nakamoto<sup>34</sup> introduced a cryptography mailing list to Bitcoin, a peer-to-peer electronic cash system “based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.” With Bitcoin, for the first time, value could be reliably transferred between two distant, untrusting parties without the need of an intermediary. Through a clever combination of cryptography and game theory, the Bitcoin ‘blockchain’—a distributed, public transaction ledger—could be used by any participant in the network to cheaply verify and settle transactions in the cryptocurrency. Thanks to rules designed to incentivize the propagation of new

legitimate transactions, to reconcile conflicting information, and to ultimately agree at regular intervals about the true state of a shared ledger (a blockchain)<sup>a</sup> in an environment where not all participating agents can be trusted, Bitcoin was also the first platform, at scale, to rely on decentralized, Internet-level ‘consensus’ for its operations. Without involving a central clearinghouse or market maker, the platform was able to settle the transfer of property rights in the underlying digital token (bitcoin) by simply combining a shared ledger with an incentive system designed to securely maintain it.

From an economics perspective, this new market design solution provides some of the advantages of a centralized digital platform (for example, the ability of participants to rely on a shared network and benefit from network effects) without some of the consequences the presence of an intermediary may introduce such as increased market power, ability to renege on commitments to ecosystem participants, control over participants’ data, and presence of a single point of failure. As a result, relative to existing financial networks, a cryptocurrency such as Bitcoin may be able to offer lower barriers to entry for new service providers and application developers, and an alternative monetary policy for

a See online appendix for more details; <https://dl.acm.org/doi/10.1145/3359552>

### » key insights

- We discuss how blockchain technology can shape innovation and competition by identifying two key costs affected by the technology: the cost of verification and the cost of networking.
- The cost of verification relates to the ability to cheaply verify state.
- The cost of networking relates to the ability to bootstrap and operate a marketplace without assigning control to a centralized intermediary. This is achieved by combining the ability to verify state with economic incentives targeted at rewarding state transitions that are particularly valuable from a network perspective.



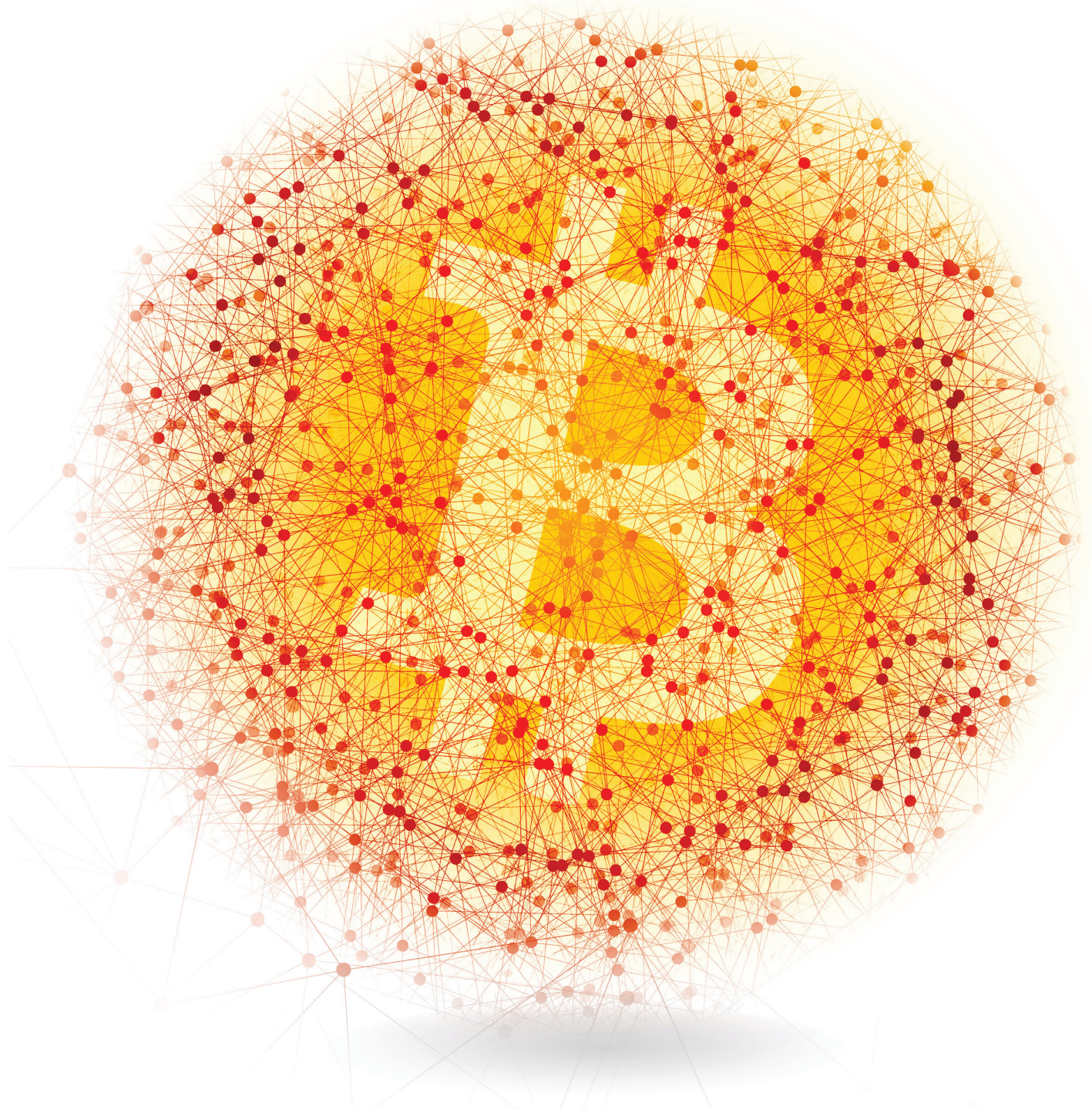


IMAGE BY ANDRÉJ BORYS ASSOCIATES

individuals that do not live in countries with trustworthy institutions. Key commitments encoded in the Bitcoin protocol are its fixed supply, predetermined release schedule, and the fact that rules can only be changed with support from a majority of participants. While the resulting ecosystem may not offer an improvement for individuals living in countries with reliable and independent central banks, it may represent an option in countries that are unable to maintain their monetary policy commitments. Of course,

the open and “permissionless” nature of the Bitcoin network, and the inability to adjust its supply also introduce new challenges, as the network can be used for illegal activity, and the value of the cryptocurrency can fluctuate wildly with changes in expectations about its future success, limiting its use as an effective medium of exchange.

In the article, we rely on economic theory to explain how two key costs affected by blockchain technology—the cost of verification of state, and the cost of networking—change the types

of transactions that can be supported in the economy. These costs have implications for the design and efficiency of digital platforms, and open opportunities for new approaches to data ownership, privacy, and licensing; monetization of digital content; auctions and reputation systems.

While the reduction in the cost of verification has economic consequences mostly on the intensive margin of production (improving existing applications), on the extensive margin (new applications), the reduction in the cost



of networking is more consequential: Bitcoin was the first digital platform to be bootstrapped in a decentralized fashion without resorting to investments by an intermediary or planner. As early adopters and investors experimented with the cryptocurrency in the hope that the network would increase in users, security<sup>b</sup> and value, the underlying token appreciated, generating the positive feedback loop needed to attract subsequent batches of users. This organic diffusion process uses high-powered incentives similar to the venture capital model to reward early adopters for taking risks and dedicating their time, effort, and capital to a new platform. The same incentive system is now used by startups to raise capital and lower switching costs for the user base and developer community of entrenched digital incumbents. This allows them to compete in a context where network effects are strongly in favor of established players.

Whereas the reduction in the cost of verification is what allows Bitcoin to settle transactions without an intermediary, the reduction in the cost of networking is what allowed its ecosystem to scale in the first place: Within eight years, the digital, scarce token native to Bitcoin went from having no value to a total market capitalization of \$180B,<sup>c</sup> and is considered by investors to be part of a new asset class and a novel type of store of value.

Beyond the idiosyncratic market design choices behind Bitcoin, the ability to track transaction attributes, settle trades, and enforce contracts across a wide variety of digital assets is what makes blockchain technology a general-purpose technology. Entries on a distributed ledger can represent ownership in currency, digital content, intellectual property, equity, information, contracts, financial and physical assets. As a result, the scaling model pioneered by Bitcoin has been adopted

by open source projects and startups interested in creating platforms for the exchange of other types of scarce, digital goods. For example, Ethereum used its own token, Ether, to bootstrap a decentralized marketplace for computing power and applications, Filecoin for data storage, BAT for digital advertising, and Blockstack for digital identity.

The new types of networks that can be created using the technology challenge the business models of incumbent digital platforms and financial institutions, and open opportunities for novel approaches to the exchange of digital assets, data ownership and monetization, information licensing, and privacy. Whereas the utopian view has argued that blockchain has the potential to transform every digital service by removing the need for intermediaries, we argue it is more likely to change the nature of intermediation by reducing the market power of intermediaries, and by progressively redefining how they add value to transactions.<sup>d</sup> This transformation will unfold slowly because even in sectors that are well-suited for a more decentralized exchange of digital assets such as finance, there are currently substantial legal and regulatory frictions to adoption. While blockchain allows for the costless verification of state when all relevant information is born digital, most markets also rely on external information—including information about identity—to ensure safe and compliant exchanges. As a result, ‘last mile’ frictions limit the conditions under which blockchain-based networks can replace existing infrastructure, as complementary innovations are needed to ensure that the shared data managed through a consensus protocol is kept in sync with critical offline information and events.

After reviewing pertinent literature, we discuss the effects of the reduction in the cost of verification, later focusing on the reduction in the cost of bootstrapping and operating a network.

<sup>d</sup> While financial intermediaries are charging high fees for cross-border payments, this revenue stream will disappear if blockchain-based payment networks commodify the transfer of value. This does not mean that intermediaries will not be able to provide added value services on top of basic payments.

## Literature

This article contributes to the nascent literature on blockchain by providing an economic framework for understanding how the technology changes the types of transactions and networks that can be sustained in the economy. By focusing on the two key economic costs the technology influences, we abstract away from some of the idiosyncratic choices different protocols make (for example, in terms of privacy, consensus algorithms, and presence of mining versus not), and surfaces high-level dimensions that have implications for market structure and competition with existing digital platforms. This level of analysis allows us to highlight commonalities between protocols that may be different at a more fine-grained technical level, but ultimately share a similar trust and competition model, and will thus have a similar impact on how rents are allocated between users, developers and nodes providing resources to a network. An online appendix (<https://dl.acm.org/doi/10.1145/3359552>) provides additional technical details on how some of the most popular cryptocurrencies work, and a taxonomy of transactions that the technology can support (for example, smart contracts, digital identity and property rights, and audit trails).

Previous research in this emerging area has focused on providing an overview of Bitcoin and its operations;<sup>7,35</sup> has combined theory and data to explain the velocity of Bitcoin and its use across countries as an investment vehicle, for gambling and illegal online markets;<sup>2</sup> and has studied the role early adopters play in the diffusion and use of Bitcoin within a large-scale, field experiment.<sup>15</sup>

Researchers have also examined competition between alternative cryptocurrencies and their differences;<sup>17,19-21</sup> the changes they entail for trading behavior;<sup>29</sup> their integration with flat-based currencies and direct use for providing citizens with central bank money;<sup>8,36,43</sup> alternative payment systems;<sup>5,42</sup> implications for regulation and governance;<sup>16,26,49,50</sup> and the privacy trade-offs cryptocurrencies and digital wallets introduce for consumers.<sup>2</sup>

From a business perspective, scholars have compared the transforma-

<sup>b</sup> In a proof-of-work blockchain, the security of the public ledger depends on the amount of computing power that is dedicated to verifying and extending the log of transactions (that is, dedicated to “mining”).

<sup>c</sup> The market capitalization is calculated as the number of tokens (approximately 16.8M bitcoin) times the value of each token (the Bitcoin to USD exchange rate was \$10,633 in January 2018; <https://coinmarketcap.com/> - accessed 01-22-2018).


tion brought about by blockchain to the introduction of communication protocols such as TCP/IP,<sup>24,25</sup> and have explored applications to digital platforms beyond finance and implications for the boundaries of the firm.<sup>10,11</sup>

### Cost of Verification

Markets facilitate the voluntary exchange of goods and services between buyers and sellers. For an exchange to be executed, key attributes of a transaction need to be verified by the parties involved. When an exchange takes place in person the buyer can usually directly assess the quality of the goods, and the seller can verify the authenticity of the cash. The only intermediary involved in this scenario is the central bank issuing and backing the fiat currency used in the exchange. When a transaction is performed online instead, one or more financial intermediaries broker it by verifying, for example, that the buyer has sufficient funds. Intermediaries add value to marketplaces by reducing information asymmetry and the risk of moral hazard through third-party verification. This often involves imposing additional disclosures, monitoring participants, maintaining trustworthy reputation systems, and enforcing contractual clauses. As markets scale in size and geographic reach, verification services become more valuable, as most parties do not have preexisting relationships, but rely on intermediaries to ensure the safety of transactions and enforce contracts. In the extreme case where verification costs are prohibitively high, markets unravel, and beneficial trades do not take place.<sup>e</sup>

In exchange for their services, intermediaries typically charge a fee. This is one of the costs buyers and sellers incur when they cannot efficiently verify all the relevant transaction attributes by themselves. Additional costs may stem from the intermediary having access to transaction data (a privacy risk) and being able to select which transactions to execute (a censorship risk).

e Over distance, intermediaries are key for verifying the quality of products or services, and reputation of buyers and sellers. High verification costs reduce market thickness<sup>39</sup> and prevent beneficial exchanges from taking place.



**Blockchain technology can prevent information leakage by allowing market participants to verify transaction attributes and enforce contracts without exposing the underlying information to a third party.**



These costs are exacerbated when intermediaries gain market power, often as a result of the informational advantage they develop over transacting parties through their intermediation services.<sup>44</sup> Transacting through an intermediary always involves some degree of disclosure to a third party, and increases the chance that the information will be later reused outside of the original contractual arrangement. Moreover, as an increasingly large share of economic and social activity is digitized, keeping data secure has become more problematic and information leakage more prevalent. Classic examples are the theft of social security numbers (for example, Equifax hack) and credit card data (for example, Target's data breach), or the licensing of customer data to advertisers. Blockchain technology can prevent information leakage by allowing market participants to verify transaction attributes and enforce contracts without exposing the underlying information to a third party.<sup>f</sup> This allows an agent to verify that some piece of information is true (for example, good credit standing), without full access to all background information (for example, past transaction records): that is, the technology allows for the verification of transaction attributes in a privacy-preserving way.

Digitization has pushed verification costs for many types of transactions close to zero. When the relevant information is digital, blockchain technology contributes to this process by allowing for costless verification.<sup>g</sup> Of course, at the interface between an offline record and its digital representation blockchain applications still face substantial frictions and “last mile” costs.<sup>45</sup> This explains why, despite claims by technology enthusiasts about the value of using the technology across a variety of applications including supply chain monitoring and digital identity, use cases outside of cryptocurrency and fintech

f This is achieved by combining a distributed ledger with zero-knowledge cryptography. Examples include cryptocurrencies such as Zcash and Zcoin.

g In practice, verification costs will never be exactly zero. What we mean by ‘costless’ is low enough to be irrelevant from an economic perspective relative to the value of the transaction.

(settings where key information and assets are digital) have been extremely limited. The link between online “on-chain” activities recorded on a blockchain and offline “off-chain” events introduces major challenges which cannot be overcome without complementary innovations. For example, a blockchain such as the Bitcoin one can be used to cheaply verify ownership and exchanges of its native digital asset. While this technically allows anyone to send and receive bitcoin globally without using an intermediary or being censored, actually being able to spend bitcoin to buy goods and services offline still runs into last mile issues. Hence, while Bitcoin has been used in countries with hyperinflation to escape devaluation, its use as a medium of exchange has been limited, and governments can still shape how these digital assets are used at the interface between the digital and the physical world. Similarly, information about identity is often used to increase the safety of market interactions, reduce fraud and build robust digital reputation systems, but being able to link an online action and digital record on a blockchain to an offline individual or entity is as expensive with blockchain technology as it would be with more traditional solutions. This drastically limits the benefits blockchain and smart contracts can bring in the absence of complementary technology (for example, a tamper-proof GPS sensor), firms and institutions that can help ensure the digital records are accurate to begin with.

The high-level process of verification is described in the accompanying figure: When a digital transaction is born, it immediately inherits some basic attributes, such as the fact that it exists and when it was created, information about the seller and buyer involved and their credentials, and so on. We typically rely on these attributes to perform subsequent actions (for example, once funds are transferred, the seller may ship the goods). Some of these actions take place every time (for example, settlement), whereas others are only triggered by specific events. A particularly interesting subset of future events are those that require additional verification. For example, a problem may emerge, and transaction attributes may need to be checked through an audit. The audit could range from actual auditors accessing the relevant logs or requesting additional information from market participants, to the execution of an internal process designed to handle the exception. Such processes tend to be costly, may involve labor and capital, and may require a third party to mediate between buyer and seller. The ideal outcome of an audit is the resolution of the problem that emerged.

Blockchain technology affects this flow by allowing, when a problem emerges, for the costless verification of digital information. Any transaction attribute or information on the agents and goods involved that is stored on a distributed ledger can be cheaply verified, in real time, by any

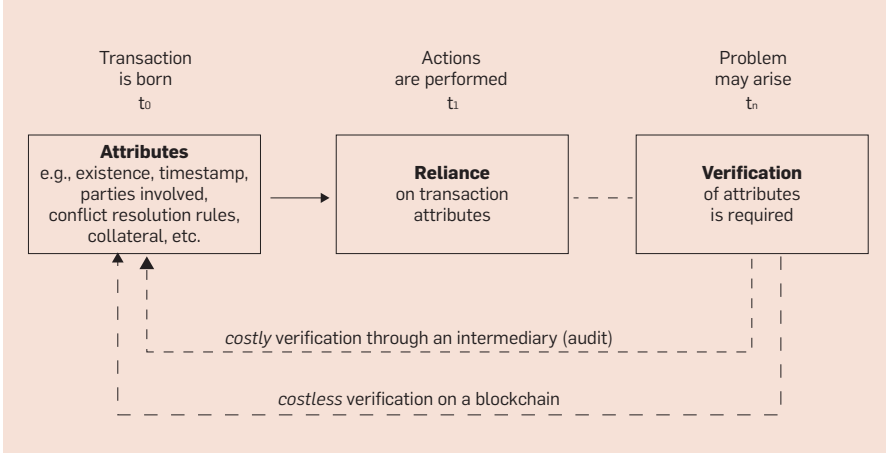
market participant. Trust in the intermediary is replaced with trust in the underlying code and consensus rules.<sup>h</sup> These rules define how a distributed network reaches agreement, at regular intervals, about the true state of the shared data it needs to maintain to operate a well-functioning marketplace. At a minimum, such shared data can represent past transactions and outstanding balances in an underlying, cryptographic token (that is, it could be a snapshot of the ownership rights in the token). In more complex applications, the shared data can also cover the rules and data required to perform a specific operation (such as, to run an application, verify that a contract clause is enforced). These operations, often referred to as “smart contracts,”<sup>i</sup> can be automated in response to new events, adding flexibility to the verification process. For example, on a shared ledger used to exchange financial assets, transacting institutions can agree, ex-ante, on the rules for the settlement and reconciliation of trades, as well as on the process they will follow and third parties they will involve if an audit is necessary or a dispute emerges. Trusted, independent oracles can also be incorporated to ensure that such financial contracts can respond to market conditions and new information (for example, to implement a weather derivative, a smart contract can aggregate information across multiple weather sources to assess if a payout has to be made).

As with past improvements in information and communication technology, reductions in the cost of verification enable the unbundling of services that were previously offered together, as part of the steps traditionally performed by an intermediary can now be delivered through a shared ledger. This allows these steps to be collectively owned and

h If we think of the audit capability of a third party as surveillance or monitoring, blockchain technology can deliver “sousveillance,”<sup>30</sup> that is, an audit embedded within the marketplace.

i N. Szabo (1996): “The basic idea of smart contracts is that many kinds of contractual clauses [...] can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive [...] for the breacher. A canonical real-life example [...] is the humble vending machine;” <https://bit.ly/2WZqMxM>

**Costly verification through an intermediary (audit) versus costless digital verification on a blockchain.**




managed by a broader group of ecosystem stakeholders, in a way that resembles collaboration among competitors and complementors in standard setting organizations,<sup>6</sup> or open source foundations. The effects of this change have been mostly felt on the intensive margin of production (that is, on improving the efficiency of pre-existing use cases), as firms are experimenting with moving different types of transactions to blockchain-based systems to reduce settlement and reconciliation costs.

As a consequence, applications resulting from the reduction in the cost of verification have been complementary to incumbents, as they improve existing value-chains by lowering the cost of tracking ownership and trading digital assets without reducing the market power of existing players. Furthermore, even when verification can be automated, intermediaries can still add value and retain influence over a market by supporting regulatory compliance, market safety, handling edge cases (for example, a chargeback), and certifying information that requires labor-intensive, offline forms of verification. This explains why implementations of the technology targeted at identity and provenance have been slower to diffuse: While the verification of digital attributes can be cheaply implemented on a blockchain, the initial mapping between offline events and their digital representations is still costly to bootstrap and maintain. Therefore, as digital verification costs fall, key complements to it that can improve the process of offline verification become more valuable.

On one extreme, blockchain technology can be used to settle trades of digital assets that are completely self-contained within a shared ledger (for example, bitcoin, ether). The consensus rules established in the code define how tokens are created and earned, and how the network reaches agreement about the true state of ownership over time.<sup>j</sup> The cost of verifying transaction attributes and enforcing



**While the verification of digital attributes can be cheaply implemented on a blockchain, the initial mapping between offline events and their digital representations is still costly to bootstrap and maintain.**



simple contracts for self-contained tokens can be extremely low. This is what allows for value to be transferred through Bitcoin across the globe at a relatively low cost. Of course, compliance with Know-Your-Customer (KYC) and Anti-Money-Laundering (AML) rules may require individuals and firms to sustain additional costs to credibly link their offline identities with their Bitcoin ones, but as long as individuals agree that the underlying token has value, using it as a store of value and medium of exchange is possible. Similarly, a native crypto token can be used to facilitate low-cost transactions of digital resources, such as computation (Ethereum), data storage (Filecoin), bandwidth, or to track equity ownership, electricity, as in all these cases verifying the exchange of a resource is not too expensive.

On the other extreme, when entries on a shared ledger are digital representations of offline identities, products, services and related transactions, costless verification is difficult to achieve. Under this scenario, the reduction in the cost of verification is contingent on maintaining a credible link between offline events and their online record. This link is cheaper to establish when offline attributes are easy to capture and expensive to alter or fake: for example, in the case of diamonds, Everledger uses the physical properties of the gems as a digital fingerprint that can be recorded and tracked on a blockchain as the products move through the supply chain. In many cases, maintaining a robust link between offline events and distributed ledgers is very expensive, and may require not only one or more trusted intermediaries, but also multiple parties to agree on rules for secure data entry and sharing. In the absence of a strong link between offline and online events, asymmetric information and moral hazard will be an issue in these markets. In this context, Internet of Things devices are instrumental in expanding the set of contracts that can be automated on a blockchain because they can be used to record real-world information (for example, through sensors and GPS devices) and substitute labor-intensive verification with inexpensive hardware.

Overall, when last-mile problems are limited—such as in the case of

<sup>j</sup> Changes in the rules are implemented through a voting process similar to standard setting negotiations, and disagreements can lead to part of the network forking to launch a platform with different market design.



digital assets that are native to a blockchain—decentralized verification goes from being costly, scarce and prone to abuse, to being cheap and reliable. While this process is unlikely to be more efficient on a per transaction basis than verification through a centralized intermediary, the ability to perform it without trusting a third party can lead to savings from increased competition, the absence of centralized control, higher privacy and censorship resistance, and the removal of single points of failure. At the same time, when frictions between offline events and their digital representations are high, these improvements are unlikely to materialize in the absence of complementary innovations, as intermediaries will still be able to control key existing complements to digital verification and use them to exert influence over market participants.

As decentralized verification becomes cheaper, the scale at which it can be efficiently implemented also drops: On a distributed ledger, data integrity can be built, from the ground up, from the most basic transaction attributes to more complex ones. For example, a robust reputation system can be constructed from the full set of interactions an economic agent has throughout the economy, increasing transparency and accountability. Expensive audits and due diligence can be progressively substituted with more frequent and fine-grained verification to ensure market safety and reduce the risk of moral hazard. A lower cost of verification also makes it easier to define property rights at a more granular scale than before, as any digital asset (or small fraction of it) can be traded, exchanged or tracked at a low cost on a shared ledger.<sup>k</sup>

### Cost of Networking

The ability to verify state (for example, the current ownership status of a digital asset) at a lower cost because of the reduction in the cost of verification allows a blockchain protocol to not only reach consensus about the history and

<sup>k</sup> In the same way that Twitter, because of the 140 character limitation, enabled new forms of communication, costless verification has the potential to change how information markets, digital property rights, and payments are designed.

## A permissionless blockchain protocol allows a network of economic agents to agree, at regular intervals, on the true state of a set of shared data without assigning residual rights to trusted entities.

proposed evolution of a digital asset, but also to define rules for state transitions that are particularly valuable from a network perspective. These transitions can be used to reward participants for performing actions that accelerate adoption and increase network value and welfare. For example, the protocol can be used to incentivize behavior that builds network effects (both in terms of users and applications), ensures the network has sufficient resources available to meet demand, guarantees its security, encourages savings or spending behavior. Taken together, these incentives lower the cost of networking, that is, the cost of bootstrapping, operating and scaling an economic network.

Whereas a reduction in the cost of verification is a necessary condition for a reduction in the cost of networking—as it is the ability to verify state that allows economic agents to establish property rights on network resources and define incentives without relying on an intermediary—it is not a sufficient condition, as implementations can take advantage of the former without the latter. In particular, when a blockchain protocol is permissioned and the entities developing it retain control over which participants can update and verify state, transitions are not fully defined by code and self-contained within the system, but rather can be influenced by external parties through fiat. As a result, from an economics perspective, the network will operate under constraints similar to those of traditional digital platforms, and participants will have to trust the platform architect and core constituents through formal and relational contracts or past reputation, among others. This tension is an important one from an organizational perspective, as it determines if a blockchain network can be considered a novel organizational form versus not.<sup>12</sup>

A permissionless blockchain protocol, instead, allows a network of economic agents to agree, at regular intervals, on the true state of a set of shared data without assigning residual rights to trusted entities. The flexibility in terms of what such shared data represents across settings (for example, currency, intellectual property, and financial assets, contracts) makes it



a general-purpose technology (GPT). GPTs typically take a long time to diffuse through the economy, but also lead to productivity gains across multiple industries.<sup>9,22,33,37</sup> Classic examples of GPTs include the steam engine, electricity, and the Internet. While permissionless networks have been compared to communication protocols such as TCP/IP—which focus on how information is packetized and routed through the Internet—they fundamentally differ from them because they allow for the secure provision, transfer and enforcement of property rights. On these networks, trust in a platform operator is replaced by trust in the underlying incentives, code and consensus rules. As a result, market power of the intermediary, privacy risk and censorship risk can be potentially reduced. The switch in the trust model also introduces new challenges, as bugs in the code can leave participants with little recourse beyond trying to coordinate a hard fork of the network. Issues with this new trust model have resulted from benign programming mistakes (such as the Parity wallet library removal),<sup>l</sup> from deliberate attempts at defrauding investors by promising high returns in the absence of any real technical or business plan (as in the case of fraudulent initial coin offerings), as well as from malicious attacks (such as the DAO hack, which led to a split of the Ethereum network).<sup>m</sup> Similarly, while blockchain protocols can be designed to offer participants a high degree of privacy (for example, Zk-Stark, Zcash, and Monero), and users can take additional measures to protect their privacy from the public (for example, using a mixing service, not reusing addresses), many shared ledgers such as the Bitcoin one are pseudonymous,<sup>n</sup> allowing third parties to deanonymize transactions and trace movements of funds over time.

Whereas permissioned networks only take advantage of the reduction in the cost of verification, permissionless ones build on the first by adding a self-

contained incentives system to also deliver a decrease in the cost of launching and operating a network without relying on trusted intermediaries. The effects of this reduction in the cost of networking are felt both in the phase of bootstrapping a new platform, and in the phase of operating it. In the first phase, a native token can be used to create incentives for adoption and to fund the development and scaling of the network, for example by having mining rewards or by raising capital through an initial coin offering (ICO). In the second phase, market design is used to define the conditions under which participants can earn tokens for contributing resources to the network (for example, computing power in the case of Bitcoin, computing and applications for Ether, disk storage for Filecoin, digital content and advertising in the case of the Basic Attention Token).

Since during the bootstrapping phase the actual utility the network can deliver to users is limited by its small scale, and network effects work against users switching from existing alternatives, this phase relies on contributions from early adopters and investors with positive expectations about the future value of the network. As in open source projects,<sup>47,48</sup> early adopters may be willing to dedicate time and effort to support a new network because they want to create a viable alternative to established products or they derive utility from advancing the underlying technology (for example, consumption utility from early access, from working on novel, complex problems, job-market signaling). Investors, instead, as in traditional equity finance, may come in early because they expect the token to appreciate in value and reward their investment.<sup>14</sup> Of course, individuals can be simultaneously early adopters and investors and contribute both effort and capital to these projects. For this set of individuals, the presence of a native token serves a similar purpose to founder and early-employee equity in startups and allows these projects to attract talent without raising investment from traditional angels and venture capitalists. Since it only takes a few lines of code to write a smart contract for an initial coin offering, open source codebases can be forked or imitated at a

low cost, and regulation is still uncertain in many jurisdictions, the ability to profit from launching a new cryptocurrency or manipulating its trading have attracted a large number of bad actors and speculators.

While lower entry barriers and the presence of technical investors could in theory open up capital for new types of entrepreneurs and ideas that traditional investors may be more reluctant to fund, the absence of regulation and oversight also allows fraudulent projects to blend in with legitimate ones and raise capital from unsophisticated investors. Combined with the fact that the value of a new token is, in most cases, purely based on expectations about its future success, and that such expectations, because of technical, regulatory and market uncertainty can rapidly turn when new information emerges or sentiment evolves, the valuations of cryptocurrencies have been extremely volatile. The resulting turmoil and speculative bubbles have made it more difficult for investors to identify high-quality projects and teams, have attracted speculators and low-quality entrants and have shifted attention from technology R&D to short-term speculative returns.

If in the first phase of growth of a blockchain-based network, incentives are predominantly targeted at accelerating adoption, in the second phase the key challenges from a market design perspective are ensuring that the incentives continue to support contributions of key resources to the ecosystem and avoiding a tragedy of the commons. By design, the protocol layer is a shared resource among all network participants, and everyone benefits from investments in it—from better security to removing technical constraints on throughput, latency or liveness. At the same time, because of the public good nature of these improvements, in the absence of proper governance, a blockchain-based network may fail to invest enough resources on them. From a valuation perspective, whereas the bootstrapping phase of a new token is associated with extremely high volatility, as uncertainty around a network's potential is resolved, it should enter a more stable growth trajectory.<sup>o</sup>

<sup>o</sup> This is similar to the process of early-stage startup funding and growth.

<sup>l</sup> See <https://bit.ly/2Uyv3GP>

<sup>m</sup> See <https://www.bloomberg.com/features/2017-the-ether-thief/>

<sup>n</sup> Like a writer writing under a pseudonym, if a Bitcoin user is ever tied to an address, the history of her transactions can be read on the blockchain.

Overall, relative to blockchain implementations that only take advantage of the reduction in the cost of verification (for example, permissioned networks), those that also benefit from the reduction in the cost of networking (for example, permissionless ones) are different on at least four dimensions. First, they are less likely to leave market power in the hands of their founders or early participants. This limits the ability of any party to unilaterally censor transactions or exclude participants from the network, and removes single points of failure, as the network does not depend on the availability of one or a few key players to operate.<sup>p</sup>

Second, they are less reliant on off-chain governance, relational contracts and laws to support their operations, as by design, to take advantage of the lower cost of networking they need to embed as much as possible of the incentives and governance rules required for their operations into the protocol. Of course, permissionless networks still need off-chain governance and coordination between their key stakeholders to execute a hard fork, implement controversial changes, or respond to an attack, but relative to more closed networks that rely on trusted intermediaries they leave less discretion to any single party, and end up codifying more of their rules into their codebases.

Third, they involve a lower privacy risk, as no single entity (or group of entities) has preferential access to or visibility over the information generated by the network.<sup>q</sup> In traditional platforms, the privacy risk is particularly salient in markets where consumers pay for services by allowing intermediaries to access and monetize their data, an issue that is increasingly relevant because of the role such data can play in the training of AI algorithms.<sup>1</sup> Whereas the trend of consumers relinquishing private information in ex-

change for free or subsidized digital services is unlikely to change because of blockchain technology—as small incentives and frictions can be used by digital platforms to persuade even privacy sensitive individuals to relinquish sensitive information<sup>2</sup>—startups in this space are experimenting with approaches that give users greater control over how, when and why their private data is accessed and monetized.

Fourth, blockchain implementations that take advantage of the lower cost of networking inevitably induce architectural changes in how firms create and capture value within markets. Architectural innovations, by destroying the usefulness of the assets and accumulated knowledge of incumbents,<sup>23</sup> open opportunities for entrants to reshape the dimensions firms compete on, and experiment with new business models. In particular, by allowing for the separation of some of the benefits of network effects from the costs of market power—since even in the absence of a platform architect participants in a blockchain network are able to rely on shared infrastructure—the technology offers new ways to reward contributors, allocate rents in a marketplace, and build applications on top of shared data while preserving the privacy of the underlying information. In traditional digital marketplaces, platform operators have wide visibility over all interactions that take place on their networks, and users are unable to directly custody or control the digital assets they use or create while transacting on them. This is a direct result of the inability of these systems to generate and trade scarce, digital assets and establish digital property rights without also assigning control over them to a third-party (usually the platform operator). Before Bitcoin, for example, a central clearing house of some type was necessary to prevent the copying and double spending of digital cash. Bitcoin solves this problem by allowing users to self-custody digital tokens and exchange them without relinquishing control over them to a third-party. This reduces switching costs between digital wallets and offers users a higher degree of privacy from service providers. Interestingly, while blockchain technology provides individuals and organizations with the opportunity to self-custody

and exchange digital assets without the need for traditional intermediaries such as banks, significant work is needed before users can reap the full benefits of this change—such as greater privacy, higher portability between service providers, and increased competition—as many implementations lack the convenience and usability of the centralized solutions consumers are used to. For example, while Bitcoin users can store and protect their own private keys, a large number of them rely on third-party wallets to do so, essentially trusting these entities with their funds as in traditional systems.

## Conclusion

The article focuses on two key costs affected by blockchain technology: the cost of verification, and the cost of networking. For markets to thrive, participants must be able to efficiently verify and audit transaction attributes, including, for example, the credentials and reputation of the parties involved, characteristics of assets exchanged, and external events and information that have implications for contractual arrangements.

Outside the boundaries of an organization, this is typically achieved by relying on trusted intermediaries. In exchange for their services, intermediaries charge fees and capitalize on their ability to observe all transactions taking place within their marketplaces. This informational advantage, combined with network effects and economies of scale, gives them substantial market power and control over market participants. Consequences of market power include higher prices, user lock-in and high switching costs, the presence of single points of failure, censorship risk, barriers to innovation, and reduced privacy.

Blockchain technology, by reducing the costs of running decentralized networks of exchange, allows for the creation of ecosystems where the benefits from network effects and shared digital infrastructure do not come at the cost of increased market power and data access by platform operators. This reduction in the cost of networking has profound consequences for market structure, as it allows open source projects and startups to directly compete with entrenched incumbents through

p The censorship risk is visible when an intermediary revokes or degrades access to a participant, and when it loses control over the marketplace because of an attack or technical failure. All three cases have been observed in online platforms, which are concentrated markets because of network effects and economies of scale in data collection, storage, and processing.

q Privacy may still be a concern if a public ledger exposes information about participants and their transactions.<sup>2</sup>


the design of platforms where the rents from direct and indirect network effects are shared more widely among participants (for example, users, application developers, and investors), and no single entity has full control over the underlying digital assets.

Because of the absence of a central clearing house or market maker, these novel networks, when permissionless, exhibit low barriers to entry and innovation. As long as applications are compatible with the rules of the protocol, they can be deployed without permission from other participants, and compete for market share. This reduces the expropriation risk application developers face when building on top of traditional digital platforms. Furthermore, since contributors can participate in governance in a way that is often proportional to their stake in the system, these networks can democratically evolve over time to accommodate changes that are beneficial to the majority of their constituents.<sup>r</sup>


From a talent acquisition perspective, unlike open source projects, the digital platforms built on top of crypto tokens do not have to rely solely on pro-social contributions of time and labor and job market signaling<sup>27</sup> to support their development. Using a native token, they can directly incentivize early contributions by developers, investors and early adopters. This novel source of funding combines crowdfunding with the simultaneous crowdsourcing of key resources needed to scale a platform and attract both developer and user activity on to it. Because of the reduction in the cost of verification, this model also allows for equity in the system to be defined at a much narrower scale, and to be allocated to a wider population of participants in response to verifiable contributions of resources.

Similarly, by allowing for the definition of scarce digital property rights, native tokens allow decentralized networks of exchange to coordinate activity around shared objectives and

r Minorities that disagree with a change face reduced lock-in because they can fork and launch a backward-compatible platform. At the same time, since forks introduce uncertainty and may decrease overall value, off-chain governance is needed to support fundamental changes in market design.



## These changes allow for the design of novel types of networks that blend features of competitive markets with the more nuanced forms of governance used within vertical integrated firms and online platforms.



transact digital resources without assigning market power to a market maker. Through blockchain-based networks, individuals and organizations can source ideas, information, capital and labor, and enforce contracts for digital assets with substantially reduced frictions. These changes allow for the design of novel types of networks that blend features of competitive markets with the more nuanced forms of governance used within vertically integrated firms and online platforms.<sup>s</sup>

Whereas intermediaries will still be able to add substantial value to transactions by focusing on tasks that are complementary to digital verification (for example, secure recording of offline events, curation, and certification of identity and services), they are likely to face increased competition because of the ability to establish and exchange digital assets on decentralized open networks without them.<sup>t</sup> This challenges some of their revenue sources and reduces their influence over markets, opening up opportunities for new business models and novel approaches to data privacy, ownership and portability, as well as to the regulation of networks that should be considered public utilities. By reducing barriers to entry within sectors that are currently heavily concentrated because of network effects and control over data, the technology may enable a new wave of innovation in digital services, and greater consumer choice.

For these changes to materialize, however, substantial hurdles will have to be overcome. First, the technology will need to reach a level of performance (for example, throughput, latency, and cost per transaction) comparable to traditional networks. While decentralization inevitably comes at a cost, the gains from greater competition, openness, privacy and censorship resistance will have to outweigh the lower efficiency of blockchain networks to make adoption worthwhile. Hybrid networks that

s For example, the hedge fund Numerai uses smart contracts to reward contributions to its financial prediction model by a distributed community of data scientists.

t Beyond financial applications, early applications that may be affected by these changes are those that involve the exchange of digital content, media, and new types of digital assets and goods.



embrace key features of permissionless systems—such as low barriers to entry and a competitive market for resources and applications—while initially borrowing trust from existing institutions to overcome scaling problems, may also provide a viable transition path when performance is an obstacle to adoption.

Second, regulatory frameworks will have to evolve to reduce uncertainty for founders and network participants, and to provide stronger protections for investors and early adopters. Because of their similarities but also their differences with equity,<sup>14</sup> crypto tokens lend themselves to both legitimate fundraising activity by high quality entrepreneurs, as well as fragrant abuse by fraudsters.<sup>13</sup> As in other technological bubbles, this constitutes a challenge for the space, as investors have a difficult time separating projects worth supporting from the much larger number of low-quality imitators, and entry by speculators has brought extreme price volatility and additional risks to the market.

Third, and possibly most important, blockchain technology, like other technological advancements, is not a panacea for every possible technical and market challenge a digital ecosystem may face. As discussed throughout this article, the technology can add substantial value under fairly narrow conditions: 1) when last mile problems are not severe and digital verification can be implemented in a novel or more fine-grained way because of a reduction in the cost of verifying state without assigning control to an intermediary; 2) when the reduction in the cost of networking allows participants to allocate rents from a digital platform more efficiently between users, developers, and investors; 3) when the combination of a reduction in both costs (verification and networking) allows for the definition of new types of digital assets and property rights; 4) when there is a need for greater privacy and ability for users to control when and how their data is accessed and used. When none of these conditions are met instead, more centralized solutions that rely on traditional intermediaries and relational contracts are unlikely to be replaced, as the benefits of transitioning to a blockchain-based system are unlikely to counterbalance the costs introduced by a decentralized

infrastructure and governance, and the replication of state across the network.

### Acknowledgments

We are thankful to Al Roth, Muneeb Ali, Naval Ravikant, Nicola Greco, Tim Simcoe, Scott Stern, Catherine Tucker, and Jane Wu for helpful discussions. ■

### References

- Agrawal, A., Gans, J., and Goldfarb, A. The simple economics of machine intelligence. *Harvard Business Rev.*, (2016), 17.
- Athey, S., Catalini, C., and Tucker, C. The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. National Bureau of Economic Research Working Paper, 2017.
- Athey, S., Parashkevov, I., Sarukkai, V., and Xia, J. Bitcoin pricing, adoption, and usage: Theory and evidence. Research paper, Stanford University, 2016.
- Ausubel, L.M. et al. The lovely but lonely Vickrey auction. *Combinatorial Auctions 17* (2006), 22–26.
- Beck, R., Czepluch, J. S., Lollike, N., and Malone, S. Blockchain—The gateway to trust-free cryptographic transactions. *ECIS*, 2016, Paper 153.
- Bekkers, R., Catalini, C., Martinelli, A., Righi, C., and Simcoe, T. Disclosure rules and declared essential patents. Discussion paper, National Bureau of Economic Research, 2019.
- Böhme, R., Christin, N., Edelman, B., and Moore, T. Bitcoin: Economics, technology, and governance. *J. Economic Perspectives* 29, 2 (2015), 213–38.
- Bordo, M.D. and Levin, A.T. Central Bank Digital Currency and the Future of Monetary Policy. National Bureau of Economic Research Working Paper, 2017.
- Bresnahan, T.F. and Trajtenberg, M. General-purpose technologies—Engines of growth? *J. Econometrics* 65, 1 (1995), 83–108.
- Catalini, C. How blockchain applications will move beyond finance. *Harvard Business Rev.*, (2017).
- Catalina, C. How blockchain technology will impact the digital economy. *Oxford Business Law Blog*, (2017).
- Catalini, C. and Bostlego, J. Blockchain Technology and Organization Science: Decentralization Theatre or Novel Organizational Form? MIT Working Paper, 2019.
- Catalini, C., Bostlego, J. and Zhang, K. Technological Opportunity, Bubbles and Innovation: The Dynamics of Initial Coin Offerings. Working Paper, 2018.
- Catalini, C. and Gans, J. S. Initial coin offerings and the value of crypto Tokens. Discussion paper. National Bureau of Economic Research, 2018.
- Catalini, C. and Tucker, C. When early adopters don't adopt. *Science*, 357, 6347 (2017), 135–136.
- Davidson, S., De Filippi, P. and Potts, J. Economics of blockchain. Working Paper, 2016.
- Dwyer, G.P. The economics of Bitcoin and similar private digital currencies. *J. Financial Stability* 17 (2015), 81–91.
- Edelman, B., Ostrovsky, M. and Schwarz, M. Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords. *Amer. Economic Rev.* 97, 1 (2007), 242–259.
- Gandal, N. and Halaburda, H. Competition in the Cryptocurrency Market. NET Institute Working Paper, 2014.
- Gans, J.S. and Halaburda, H. Some economics of private digital currency. *Economic Analysis of the Digital Economy*, (2015), 257–276. University of Chicago Press.
- Halaburda, H. and Sarvary, M. *Beyond Bitcoin: The Economics of Digital Currencies*. Springer, 2016.
- Helpman, E. *General Purpose Technologies and Economic Growth*. MIT Press, Cambridge, MA, 1998.
- Henderson, R.M. and Clark, K.B. Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms. *Administrative Science Q.* (1990), 9–30.
- Iansiti, M. and Lakhani, K.R. The truth about blockchain. *Harvard Business Rev.* 95, 1 (2017), 118–127.
- Ito, J., Narula, N. and Ali, R. The blockchain will do to the financial system what the Internet did to media. *Harvard Business Rev.* (2017)
- Kiviat, T.I. Beyond bitcoin: Issues in regulating blockchain transactions. *Duke LJ* 65, 569 (2015).
- Lerner, J. and Tirole, J. Some simple economics of open source. *J. Industrial Economics* 50, 2 (2002), 197–234.
- Luca, M. Designing online marketplaces: Trust and

- reputation mechanisms. *Innovation Policy and the Economy* 17, 1 (2017), 77–93.
- Malinova, K. and Park, A. Market Design with Blockchain Technology. Working Paper, 2016.
  - Mann, S., Nolan, J. and Wellman, B. Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society* 1, 3 (2002), 331–355.
  - Milgrom, P.R. *Putting auction theory to work*. Cambridge University Press, 2004.
  - Morton, F.S. Consumer benefit from use of the Internet. *Innovation Policy and the Economy* 6 (2006), 67–90.
  - Moser, P. and Nicholas, T. Was electricity a general-purpose technology? Evidence from historical patent citations. *Amer. Economic Rev.* 94, 2 (2004), 388–394.
  - Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008.
  - Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press, 2016.
  - Raskin, M., and Yermack, D. Digital currencies, decentralized ledgers, and the future of central banking. National Bureau of Economic Research Working Paper, 2016.
  - Rosenberg, N. and Trajtenberg, M. A general-purpose technology at work: The Cortiss steam engine in the late 19<sup>th</sup> century US. National Bureau of Economic Research Working Paper, 2001.
  - Roth, A.E. The economist as engineer: Game theory, experimentation, and computation as tools for design economics. *Econometrica* 70, 4 (2002), 1341–1378.
  - Roth, A.E. The art of designing markets. *Harvard Business Rev.* 85, 10 (2007), 118.
  - Roth, A.E., and Ockenfels, A. Last-minute bidding and the rules for ending second-price auctions: Evidence from eBay and Amazon auctions on the Internet. *Amer. Economic Rev.* 92, 4 (2002), 1093–1103.
  - Rothkopf, M.H., Teisberg, T.J., and Kahn, E.P. Why are Vickrey auctions rare? *J. Political Economy* 98, 1 (1990), 94–109.
  - Rysman, M., and Schuh, S. New innovations in payments. *Innovation Policy and the Economy* 17, 1 (2017), 27–48.
  - Seretakis, A. Blockchain, Securities Markets and Central Banking. Working Paper, 2017.
  - Stiglitz, J.E. Information and the change in the paradigm in economics. *Amer. Economic Rev.* 92, 3 (2002), 460–501.
  - Tucker, C. and Catalini, C. What blockchain can't do. *Harvard Business Rev.* (2018).
  - Von Hippel, E. *Democratizing Innovation*. MIT Press, 2005.
  - Von Hippel, E.A. Open source projects as horizontal innovation networks—by and for users. 2002.
  - Von Hippel, E. and Von Krogh, G. Open source software and the private collective innovation model: Issues for organization science. *Organization Science* 14, 2 (2003), 209–223.
  - Walport, M. Distributed ledger technology: Beyond block chain. U.K. Government Office for Science, 2016.
  - Wright, A. and De Filippi, P. Decentralized blockchain technology and the rise of lex cryptographia. 2015.

**Christian Catalini** (catalini@mit.edu) is the Theodore T. Miller Career Development Professor at MIT, associate professor of Technological Innovation, Entrepreneurship, and Strategic Management at the MIT Sloan School of Management, and founder of MIT Cryptoeconomics Lab, Cambridge, MA, USA.

**Joshua S. Gans** (joshua.gans@rotman.utoronto.ca) is a professor of strategic management and holder of the Jeffrey Skoll Chair in Technical Innovation and Entrepreneurship at the Rotman School of Management, University of Toronto, CA.

Copyright held by authors/owners.



Watch the authors discuss this work in this exclusive *Communications* video. <https://cacm.acm.org/videos/economics-of-the-blockchain>