Some Simple Economics of the Blockchain

Christian Catalini (MIT) and Joshua S. Gans (University of Toronto)*

September 21, 2017

Abstract

We rely on economic theory to discuss how blockchain technology will shape the rate and direction of innovation. We identify two key costs affected by the technology: 1) the cost of verification; and 2) the cost of networking. The first cost relates to the ability to cheaply verify the attributes of a transaction. The second one to the ability to bootstrap and operate a marketplace without the need for a traditional intermediary: When combined with a native token (as in Bitcoin and Ethereum), a blockchain allows a decentralized network of economic agents to agree, at regular intervals, about the true state of shared data. This shared data can represent exchanges of currency, intellectual property, equity, information or other types of contracts and digital assets - making blockchain a general purpose technology that can be used to trade scarce, digital property rights and create novel types of digital platforms. The resulting marketplaces are characterized by increased competition, lower barriers to entry and innovation, lower privacy and censorship risk, and allow participants within the same ecosystem to make investments to support and operate shared infrastructure without assigning market power to a platform operator. They also challenge the existing revenue models and accumulated knowledge and resources of incumbents, and open opportunities for new approaches to startup fundraising, the provision of public goods and software protocols, data ownership and licensing, auctions and reputation systems.

Keywords: blockchain, cryptocurrency, market design, tokens, initial coin offerings, smart contracts, distributed ledgers, Bitcoin, Ethereum, open source, auctions.

*Christian Catalini is the Theodore T. Miller Career Development Professor at MIT, Assistant Professor of Technological Innovation, Entrepreneurship, and Strategic Management at the MIT Sloan School of Management: catalini@mit.edu. Joshua S. Gans 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: joshua.gans@rotman.utoronto.ca. We are thankful to Al Roth, Muneeb Ali, Naval Ravikant, Nicola Greco, Tim Simcoe, Scott Stern, Catherine Tucker, Jane Wu for helpful discussions.

1 Introduction

In October 2008, a few weeks after the Emergency Economic Stabilization Act rescued the U.S. financial system from collapse, Satoshi Nakamoto (Nakamoto 2008) 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 in history, 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')[1] 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 - which was subsequently adopted and extended by other types of digital platforms – removes the costs arising from the presence of a single platform operator, while still allowing marketplace participants to access and use shared infrastructure, and transact with each other.

In the paper, we rely on economic theory to explain how two key costs affected by blockchain technology – the *cost of verification* of transaction attributes, and the *cost of networking* – change the types of transactions that can be supported in the economy. While

[1] See Appendix for more details.

the reduction in the cost of verification has economic consequences mostly on the intensive margin of production, on the extensive margin, 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[2] 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 contributors for taking risks and dedicating their time, effort, and capital to a new platform. The same incentive system is now used by entrants to raise capital and lower switching costs for the user base and developer community of entrenched 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 the platform 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 $75B,[3] and is considered by investors part of a new asset class both as a digital store of value, and a medium of exchange.[4]

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

[2]In a proof-of-work blockchain such as the one used by Bitcoin, the security of the public ledger depends on the amount of computing power that is dedicated to verifying and extending the log of transactions over time (i.e. that is dedicated to "mining").

[3]The market capitalization is calculated as the number of tokens in circulation (approximately 16.5M bitcoin) times the value of each token (the Bitcoin to USD exchange rate was $4360 in August 2017). The second largest cryptocurrency, Ethereum, had a $30B market cap (source: https://coinmarketcap.com/ - accessed 09-06-2017).

[4]While money, in addition to being a valid store of value and medium of exchange, also needs to be a valid unit of account, in a digital environment this is irrelevant, as value can be cheaply visualized in the currency of choice of the user.

is what makes blockchain technology a general purpose technology. Entries on a distributed ledger can represent ownership in currency, 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 attention, Blockstack for digital identity etc.

The resulting marketplaces challenge the existing revenue models of incumbents, and open opportunities for novel approaches to data ownership, and the provision of goods and services online. Whereas the utopian view has argued that blockchain technology will affect every market by removing the need for intermediaries, we argue that it is more likely to change the nature of intermediation. Furthermore, for the technology to have any impact in a specific market, verification of transaction attributes and contracts needs to be currently expensive, platform operators must be enjoying uncompetitive rents from their position as trusted nodes above and beyond their added value to transactions, or the privacy risk and censorship risk must be substantial.

The paper proceeds as follows: We first review the literature in Section 1.1. In Section 2, we discuss the effects of the reduction in the cost of verification. Section 3 focuses on the reduction in the cost of bootstrapping and operating a network. Section 4 concludes.

1.1 Literature

The paper contributes to the nascent literature on cryptocurrencies and blockchain by providing an economic framework for understanding how the technology changes the types of transactions and platforms that can be sustained in the economy. Whereas there are many different implementations of blockchain technology, for the purpose of this paper we abstract away from their idiosyncratic features and focus on the high-level, shared dimensions that

have implications for market design. In the Appendix, we provide additional technical details on how cryptocurrencies and distributed ledgers work, as well as a taxonomy of transaction types that can be supported through the technology (e.g. central bank money, auctions, smart contracts, digital identity and property rights, audit trails etc).

Previous research in this emerging area has focused on providing an overview of Bitcoin and its operations (Yermack 2013, Böhme, Christin, Edelman, and Moore 2015, Narayanan, Bonneau, Felten, Miller, and Goldfeder 2016); 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 (Athey, Parashkevov, Sarukkai, and Xia 2016); and has studied the role early adopters play in the diffusion and use of Bitcoin within a large-scale, field experiment (Catalini and Tucker 2017).

Researchers have also examined competition between alternative cryptocurrencies and their differences (Gandal and Halaburda 2014, Gans and Halaburda 2015, Dwyer 2015, Halaburda and Sarvary 2016); the changes they entail for trading behavior (Malinova and Park 2016); their integration with fiat-based currencies and direct use for providing citizens with central bank money (Raskin and Yermack 2016, Seretakis 2017, Bordo and Levin 2017) and alternative payment systems (Beck, Czepluch, Lollike, and Malone 2016, Rysman and Schuh 2017); implications for regulation and governance (Wright and De Filippi 2015, Davidson, De Filippi, and Potts 2016, Kiviat 2015, Walport 2016); and the privacy trade-offs cryptocurrencies and digital wallets introduce for consumers (Athey, Catalini, and Tucker 2017).

From a business perspective, scholars have compared the transformation brought about by blockchain to the introduction of communication protocols such as TCP/IP (Iansiti and Lakhani 2017, Ito, Narula, and Ali 2017), and have explored applications to digital platforms beyond finance and implications for the boundaries of the firm (Catalini 2017a, Catalini 2017b).

2 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 contract 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.

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).

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 (Stiglitz 2002). 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 (e.g. Equifax hack) and credit card data (e.g. Target data breach), or the resale 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.[5] This allows an agent to verify that some piece of information is true (e.g. good credit standing), without full access to all background information (e.g. past transaction records): i.e., 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. Blockchain technology completes this process by allowing for *costless verification*.[6] At scale, a blockchain such as the Bitcoin one, can be used to cheaply verify ownership and exchanges in the cryptocurrency. While the Bitcoin network consumes computing power to secure transactions and extend its distributed ledger, it is important to highlight that such energy requirement is small compared to the costs of labor and capital involved in securing transactions on traditional financial infrastructure.[7] Furthermore, whereas in existing payment platforms intermediaries have access to all transaction data and accumulate market power, this is not the case on a blockchain-based system, as low barriers to entry and innovation, combined with the ability to fork the underlying code, ensure a higher level of competition for different types of services.

The high-level process of verification is described in Figure 1: When a transaction is born in the economy, it immediately inherits some basic attributes, such as the fact that it

[5]This is achieved by combining a distributed ledger with zero-knowledge cryptography. Examples include cryptocurrencies such as Zcash and Zcoin (which respectively have $460M and $25M market capitalization.

[6]Of course, 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.

[7]This also has a competitive element. See (Ma, Gans, and Tourky 2017) for more details.

exists and when it was created, information about the seller and buyer involved and their credentials, etc. We typically rely on these attributes to perform subsequent actions (e.g., once funds are transferred, the seller may ship the goods). Some of these actions take place every time (e.g. 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. Often such processes are costly, involve both 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.

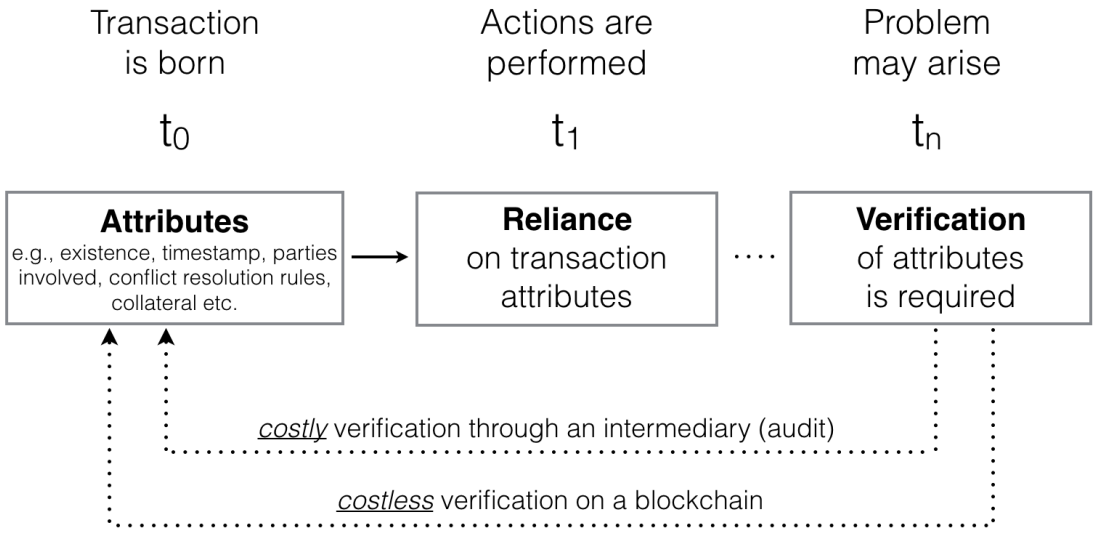

Figure 1: Costly Verification Through an Intermediary (Audit) versus Costless Verification on a Blockchain

Blockchain technology fundamentally transforms this flow by allowing, when a problem emerges, for costless verification. 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

market participants. Trust in the intermediary is replaced with trust in the underlying code and consensus rules.[8] These rules define how a distributed network can reach 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 underling, cryptographic token (i.e. it could be a snapshot of the ownership rights in the token). In more complex platforms, the shared data can also cover the code and data required to perform a specific operation (i.e. to run an application, verify that a contract clause is enforced). These operations, often referred to as 'smart contracts',[9] can be automated in response to future events, adding substantial flexibility to the process of verification. For example, transacting parties can agree, ex-ante, on the rules for an audit, further reducing the need for dispute resolution if a problem emerges. Trusted, independent sources of information, can also be incorporated in the process. For example, if buyer and seller agreed to different terms based on the weather conditions, a smart contract could aggregate information from multiple weather sources (including sensors) to adjudicate a dispute.

The reduction in the cost of verification has started the unbundling of verification services, as some of the tasks traditionally performed by an intermediary can now be delivered at a lower cost through blockchain technology. The effects of this change have been mostly felt on

[8] If we think of the audit capability of the third-party that intervenes when a problem emerges in a traditional market as surveillance or monitoring, blockchain technology can deliver "sousveillance" (Mann, Nolan, and Wellman 2002), i.e. an audit that is embedded within the rules of the marketplace.

[9] In 1996, Nick Szabo defined smart contracts as: *"The basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a beginner's level problem in design with finite automata, dispense change and product fairly. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, proactively enforced form, and provide much better observation and verification where proactive measures must fall short."* Source: `http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html`

the intensive margin of production and for digital assets, as established players have moved existing types of transactions onto blockchain-based systems to lower operation costs. Ripple, for example, uses the technology to allow for cheaper, cross-border payments in fiat-currency between existing banks; Digital Asset and Chain are using the same approach to enable more efficient trades of financial assets; Western Union has invested in the space to lower costs in the remittances market; Abra and Circle use the technology for global, peer-to-peer payments in fiat-currencies; NASDAQ deployed a solution to track equity in privately held companies; the state of Delaware is moving incorporation data on a distributed ledger, etc.

Applications resulting from the reduction in the cost of verification have been mostly complementary to incumbents, as they improve existing value-chains by lowering the cost of settlement and reconciliation of transactions. Moreover, although many verification steps can now be commoditized, intermediaries are still needed for providing a user-friendly experience, handling edge cases (e.g. a chargeback, the enforcement of an escrow contract), and for 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 entities and their digital representations is still costly to bootstrap and maintain. Therefore, as verification costs fall, this key complement to digital verification becomes more valuable.

On one extreme, blockchain technology can be used to settle trades of digital, scarce goods that are completely self-contained within a platform (e.g. bitcoin, ether). The consensus rules established in the code define how tokens are earned, and how the network reaches agreement about the true state of ownership in the tokens over time.[10] The cost of verifying transaction attributes and enforcing simple contracts for self-contained tokens is practically

[10]Changes in the rules are implemented though a voting process similar to standard setting negotiations, and disagreement can lead to part of the network forking the codebase and current state of the distributed ledger and launch a competing platform with different market design rules.

zero. This is what allows for value to be transferred through Bitcoin across the globe at very 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 medium of exchange is extremely cheap. Similarly, a crypto token can be used to facilitate low cost transactions of digital resources such as computation (Ethereum), data storage (Filecoin), bandwidth or electricity, as in all these cases verifying attributes of transactions is easy.

On the other extreme, when entries on a distributed ledger are digital representations of offline identities, products, services and related transactions, costless verification is more 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: e.g., 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 still expensive, and may require not only one or more trusted intermediaries, but often also multiple parties within the same ecosystem 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 still 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 (e.g. through sensors, GPS devices etc.) and substitute labor intensive verification with inexpensive hardware.

Overall, for transaction attributes that can be reliably recorded on a blockchain, verification goes from being costly, scarce and prone to abuse, to being cheap and reliable. As

a consequence, we will see more verification and smart contracts in the economy, and a key complement to verification – the secure recording of offline transaction attributes through devices or intermediaries – will become more valuable. Moreover, as verification becomes cheaper, the scale at which it can be efficiently implemented drops: On a distributed ledger, data integrity can be built, from the ground up, from the most basic transaction attributes to the most complex ones. For example, a robust reputation and identity system can be constructed from the full set of interactions an economic agent has throughout the economy. This makes it substantially harder to alter or fake attributes of transactions for the entities involved (e.g. voting machines, accounting records, etc.). What previously constituted a time consuming and costly audit, is now a process that can run continuously in the background to ensure market safety and compliance, lowering the risk of moral hazard.

The shift also makes it easier to define property rights at a smaller scale than before, as any digital asset (or small fractions of it) can be easily traded, exchanged and verified at a low cost. In the same way that Twitter, because of the 140 character limitation, enabled new forms of communication, the ability to implement costless verification at the level of a single bit of information will fundamentally change how information markets, contracts and digital property rights are designed.

3 Cost of Networking

Blockchain technology allows a network of economic agents to agree, at regular intervals, on the true state of shared data. The flexibility in terms of what such shared data represents across settings (e.g. currency, intellectual property, financial assets, contracts etc.) 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 (Bresnahan and Trajtenberg 1995, Helpman 1998, Rosenberg and Trajtenberg 2001, Moser and Nicholas

2004). Classic examples of GPTs include the steam engine, electricity, and the internet.

While blockchain technology is often compared to communication protocols such as TCP/IP – which focuses on how *information* is packetized and routed through the internet – it fundamentally differs from them because it allows for the secure transfer and enforcement of *property rights*. This enables the creation of new types of platforms where the exchange and provision of digital assets does not rely on an intermediary. On these platforms, 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 are drastically reduced. This is possible because blockchain technology decreases the cost of networking.

The effects of the 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 – often referred as a token sale or Initial Coin Offering (ICO) – a native token is used to crowdfund the development of a platform. In the second phase, an incentive system is used to determine the conditions under which contributors can earn tokens for providing the resources needed for the platform's operations (e.g. computing power in the case of Bitcoin, applications for Ether, storage for Filecoin, content and advertising in the case of the Basic Attention Token, etc.).

Since during the bootstrapping phase the actual utility the platform can deliver to users is limited by its small scale and network effects work against users switching from existing solutions, this first phase relies on contributions by early adopters and expectations about the future value of the ecosystem by investors. As in open source projects (Von Hippel 2002, Von Hippel and Von Krogh 2003, Von Hippel 2005), early adopters may be willing to dedicate time and effort to support a new platform because they want to create a viable alternative to established products and derive utility from developing the technology further (e.g. consumption utility from early access, from working on novel, complex problems, job-

market signalling). Investors instead – as in traditional early-stage capital markets – come in early because they expect the token to appreciate in value and reward their investment. Of course, many individuals are simultaneously early adopters and investors, i.e. they 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 top global talent without raising investment from traditional angels and venture capitalists.

The second phase of growth requires mainstream users to have joined the platform because it creates value for them or their business. This early majority is indifferent to the technological details of the solution adopted, and cares about the potential of the technology to make existing processes cheaper or new ones possible. Whereas the bootstrapping phase is associated with extremely high volatility, as uncertainty around a platform's potential is resolved, tokens enter a more stable growth trajectory. This is similar to the process of early-stage startup funding and growth. Within the cryptocurrency space, token sales and ICOs have substantially shortened the time it takes for a developer team to raise capital, and for a new token to reach a critical mass of early adopters and investors. While Bitcoin, which was bootstrapped through a slow process of word-of-mouth within the cypherpunk community, took four years to reach a $1B market cap, Ethereum took only two years to reach the same milestone.

The reduction in the cost of networking – because of its effects on market power, privacy risk and censorship risk – constitutes an architectural change to value creation and capture. Architectural innovations, by destroying the usefulness of the knowledge and assets incumbents have accumulated (Henderson and Clark 1990), open opportunities for entrants to reshape market structure. In the case of blockchain, by reducing the market power of intermediaries, the technology also allows platforms to operate with lower barriers to entry and innovation. Whereas we had the ability to crowdsource ideas, talent and capital online

for multiple years, existing solutions rely on a central clearinghouse to match demand and supply, maintain reputation systems and trust, and ultimately ensure the safety of transactions. The open innovation protocols that can be built using a crypto token, instead, enable the creation of platforms where rents are more equally distributed among contributors, consumers do not have to expose their private data to a single intermediary, and a broader segment of developers and users can benefit from the returns to direct and indirect network effects the use of a shared standard (and infrastructure) generates.

In the current model, most consumers and businesses are renting resources on the internet, and do not own or control the digital and financial assets they rely on every day. This is the result of our inability to generate and trade scarce, digital goods and establish digital property rights without an intermediary (including the government). Before Bitcoin, any form of digital cash, like other digital goods, could be easily copied and double spent, making the system worthless in the absence of a central clearinghouse. Crypto tokens solve this problem by allowing for the creation and exchange of scarce, digital assets without the negative effects stemming from assigning market power to a third-party. The consequences of market power in these digital markets, including financial ones, range from higher prices and switching costs to higher privacy and censorship risk.

The privacy risk is particularly salient in markets where consumers pay for services by allowing intermediaries to mine their personal data. With the rise of machine intelligence (Agrawal, Gans, and Goldfarb 2016), access to data can reinforce market power, as incumbents increasingly compete on developing and training the most effective prediction algorithms. The trend of consumers relinquishing private information in exchange for free or subsidized digital services is unlikely to change, as small incentives, frictions in navigation and irrelevant information can all be used by intermediaries to persuade even privacy sensitive individuals to give up sensitive information (Athey, Catalini, and Tucker 2017). Nevertheless, startups such as the BAT (online content and advertising) and Blockstack

(decentralized identity and applications) have launched crypto tokens targeted at increasing consumers' ability to control how, when and why their private data is accessed and monetized. If successful, the resulting platforms would shift us from a context where intermediary pledge to 'not be evil', to one where they 'can't be evil' in the first place.[11]

The censorship risk is visible when an intermediary *revokes* a participant's access to the marketplace and digital assets through fiat as in online censorship; when it *degrades* access (e.g. in terms of speed, features etc.) to some participants to reduce their ability to effectively compete; and when it *loses* control over the marketplace because of an attack or technical failure. All three cases have been observed in online platforms (e.g. Amazon Cloud Services, Google's Search and AdSense, Facebook etc.), which are heavily concentrated markets because of network effects and economies of scale in data collection, storage, and processing. This not only gives additional market power to a small number of entrenched incumbents, but also makes the underlying services less resilient to targeted attacks and errors.[12] Promising solutions to these problems are being deployed by startups such as Filecoin, which is attempting to turn data storage and transfer into a commodity, and through blockchain-based distributed computing platforms such as Ethereum.

4 Conclusions

The paper focuses on two key costs that are affected by blockchain technology: the cost of verification, and the cost of networking. For markets to thrive, participants need to be able to efficiently verify and audit transaction attributes, including the credentials and reputation of the parties involved, the characteristics of the goods and services exchanged, future events that have implications for contractual arrangements, etc.

Outside the boundaries of an organization, this is achieved within the current paradigm

[11] https://medium.com/@muneeb/cant-be-evil-bc5ec16c6306

[12] https://www.technologyreview.com/s/603784/amazons-150-million-typo-is-a-lightning-rod-for-a-big-cloud-problem/

by relying on third-party intermediaries. In exchange for their services, intermediaries typically charge a fee or monetize their ability to observe all transactions taking place within a marketplace. This informational advantage, combined with network effects and economies of scale, often gives them substantial market power. Consequences of market power include higher prices, lock-in, the presence of a single point of failure, reduced innovation, privacy risk and censorship risk.

Blockchain technology, by drastically reducing the cost of running decentralized networks of exchange, enables the creation of digital platforms where the benefits from network effects and shared digital infrastructure do not come at the cost of increased market power and data access by an intermediary. This reduction in the cost of networking has profound consequences for market structure, as it allows startups and open-source projects to directly compete with entrenched incumbents through the design of platforms where the rents from direct and indirect network effects are shared more widely among participants (e.g. developers, users, investors), and no single player has full control over the underlying digital assets and data.

Because of the absence of a central 'clearing house' or market maker, these novel digital platforms also allow for permissionless innovation: As long as an application is compatible with the established protocol and consensus rules, it can be deployed on the network without permission from other participants. This reduces the expropriation risk application developers face when building on top of existing digital platforms (e.g. iOS, Facebook etc.). Furthermore, since each contributor to a blockchain-based platform can theoretically shape its evolution in a way that is proportional to its stake in the platform (e.g. in terms of computing power, storage, labor or capital dedicated to it), these new platforms can democratically evolve over time to accommodate changes in market design that are beneficial to the majority of contributors. Minorities that disagree with a proposed change face reduced lock-in and hold-up risk because they can fork the existing codebase at any time and launch

a separate, backwards-compatible platform under their preferred rules. At the same time, since forks introduce uncertainty and a network split may decrease the overall value of a platform, better forms of governance are needed to allow decentralized communities of developers and users to reach agreement about fundamental changes to market design without destroying confidence in the ecosystem.

From a talent perspective, unlike open source projects, the digital platforms built on top of a crypto token do not have to only rely on job market signalling (Lerner and Tirole 2002), and pro-social contributions of time and labor to support their development. They also do not need capital from traditional investors to fund their growth, although they may need their expertise and connections to scale and grow their business. They can also reward and attract early adopters in novel ways. By embedding a native token in their operations, these ecosystems can directly incentivize early contributions by developers, investors and users by allocating them a disproportionate share of equity in the platform. This novel form of equity crowdfunding combines online capital fundraising with the simultaneous crowdsourcing of key resources needed to scale a platform and attract activity on it both on the developer and the user side. Because of the reduction in the cost of verification, this model improves on the venture capital and angel-investor one by allowing for equity to be efficiently and automatically distributed in substantially smaller fractions, to a wider population of individuals, and in response to verifiable contributions of resources.

This approach to scaling startups and open source projects radically changes the funding of innovation, provision of public goods and software, and the overall operations of digital platforms. By allowing for the definition of scarce, digital property rights, it also allows a decentralized network of economic agents to coordinate around a shared objective and transact resources without assigning market power to an intermediary. Through blockchain-based platforms, individuals and organizations can source ideas, capital and labor, and enforce contracts for digital goods and services on a global scale with substantially reduced

frictions. These changes also allow for the design of novel types of organizations that blend features of competitive markets with the more nuanced forms of governance used within vertically integrated firms and online platforms. For example, the hedge fund Numerai uses smart contracts to transparently reward contributions to its financial prediction models: Data scientists across the globe can collaborate through this new type of digital platform knowing that their inputs will be rewarded – using the native, Numeraire token – according to their impact on the ultimate performance of the hedge fund.

Whereas intermediaries can still add substantial value to transactions by focusing on tasks that are complementary to digital forms of verification (e.g. secure recording of offline events and attributes on a blockchain, curation and certification services etc), they are likely to face increased competition because of the ability to cheaply establish and trade digital assets on open, permissionless digital platforms without them. This challenges their existing revenue models and market power, and opens opportunities for fundamentally new business models and approaches to data privacy, ownership and portability, as well as government regulation of digital marketplaces.[13] By reducing barriers to entry within sectors that are currently heavily concentrated because of network effects and control over data, blockchain technology has also the potential to enable a new wave of innovation in digital marketplaces.

[13]From a regulatory perspective, the transparency enabled by blockchain technology also allows regulators to closely monitor market participants on a regular basis and costlessly verify the integrity of their actions through digital audit trails.

References

Agrawal, A., J. Gans, and A. Goldfarb (2016): "The simple economics of machine intelligence," *Harvard Business Review*, 17.

Athey, S., C. Catalini, and C. Tucker (2017): "The Digital Privacy Paradox: Small Money, Small Costs, Small Talk," *National Bureau of Economic Research Working Paper*.

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia (2016): "Bitcoin pricing, adoption, and usage: Theory and evidence," .

Ausubel, L. M., P. Milgrom, et al. (2006): "The lovely but lonely Vickrey auction," *Combinatorial auctions*, 17, 22–26.

Beck, R., J. S. Czepluch, N. Lollike, and S. Malone (2016): "Blockchain-the Gateway to Trust-Free Cryptographic Transactions.," in *ECIS*, p. ResearchPaper153.

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

Bordo, M. D., and A. T. Levin (2017): "Central Bank Digital Currency and the Future of Monetary Policy," *National Bureau of Economic Research Working Paper*.

Bresnahan, T. F., and M. Trajtenberg (1995): "General purpose technologies Engines of growth?," *Journal of econometrics*, 65(1), 83–108.

Catalini, C. (2017a): "How Blockchain Applications Will Move Beyond Finance," *Harvard Business Review*.

——— (2017b): "How Blockchain Technology Will Impact the Digital Economy," *Oxford Business Law Blog*.

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

Davidson, S., P. De Filippi, and J. Potts (2016): "Economics of blockchain," *Working Paper*.

Dwyer, G. P. (2015): "The economics of Bitcoin and similar private digital currencies," *Journal of Financial Stability*, 17, 81–91.

Edelman, B., M. Ostrovsky, and M. Schwarz (2007): "Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords," *American Economic Review*, 97(1), 242–259.

Gandal, N., and H. Halaburda (2014): "Competition in the Cryptocurrency Market," *NET Institute Working Paper*.

Gans, J. S., and H. Halaburda (2015): "Some economics of private digital currency," in *Economic Analysis of the Digital Economy*, pp. 257–276. University of Chicago Press.

Halaburda, H., and M. Sarvary (2016): *Beyond bitcoin: The economics of digital currencies*. Springer.

Helpman, E. (1998): *General purpose technologies and economic growth*. MIT press.

Henderson, R. M., and K. B. Clark (1990): "Architectural innovation: The reconfiguration of existing product technologies and the failure of established firms," *Administrative science quarterly*, pp. 9–30.

Iansiti, M., and K. R. Lakhani (2017): "The Truth About Blockchain," *Harvard Business Review*, 95(1), 118–127.

Ito, J., N. Narula, and R. Ali (2017): "The Blockchain Will Do to the Financial System What the Internet Did to Media," *Harvard Business Review*.

Kiviat, T. I. (2015): "Beyond Bitcoin: Issues in Regulating Blockchain Tranactions," *Duke LJ*, 65, 569.

Lerner, J., and J. Tirole (2002): "Some simple economics of open source," *The journal of industrial economics*, 50(2), 197–234.

Luca, M. (2017): "Designing Online Marketplaces: Trust and Reputation Mechanisms," *Innovation Policy and the Economy*, 17(1), 77–93.

Ma, J., J. S. Gans, and R. Tourky (2017): "Market Structure in Bitcoin Mining," *mimeo, ANU*.

Malinova, K., and A. Park (2016): "Market Design with Blockchain Technology," *Working Paper*.

Mann, S., J. Nolan, and B. Wellman (2002): "Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments.," *Surveillance & society*, 1(3), 331–355.

Milgrom, P. R. (2004): *Putting auction theory to work*. Cambridge University Press.

Moser, P., and T. Nicholas (2004): "Was electricity a general purpose technology? Evidence from historical patent citations," *The American Economic Review*, 94(2), 388–394.

Nakamoto, S. (2008): "Bitcoin: A peer-to-peer electronic cash system," *White Paper*.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016): *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

Raskin, M., and D. Yermack (2016): "Digital currencies, decentralized ledgers, and the future of central banking," *National Bureau of Economic Research Working Paper*.

Rosenberg, N., and M. Trajtenberg (2001): "A General purpose technology at work: the Corliss steam engine in the late 19th Century US," *National Bureau of Economic Research Working Paper*.

Roth, A. E. (2002): "The economist as engineer: Game theory, experimentation, and computation as tools for design economics," *Econometrica*, 70(4), 1341–1378.

Roth, A. E., and A. Ockenfels (2002): "Last-minute bidding and the rules for ending second-price auctions: Evidence from eBay and Amazon auctions on the Internet," *The American Economic Review*, 92(4), 1093–1103.

Rothkopf, M. H., T. J. Teisberg, and E. P. Kahn (1990): "Why are Vickrey auctions rare?," *Journal of Political Economy*, 98(1), 94–109.

Rysman, M., and S. Schuh (2017): "New innovations in payments," *Innovation Policy and the Economy*, 17(1), 27–48.

Seretakis, A. (2017): "Blockchain, Securities Markets and Central Banking," *Working Paper*.

Stiglitz, J. E. (2002): "Information and the Change in the Paradigm in Economics," *The American Economic Review*, 92(3), 460–501.

Von Hippel, E. (2005): *Democratizing innovation*. MIT press.

Von Hippel, E., and G. Von Krogh (2003): "Open source software and the private-collective innovation model: Issues for organization science," *Organization science*, 14(2), 209–223.

Von Hippel, E. A. (2002): "Open source projects as horizontal innovation networks-by and for users," .

Walport, M. (2016): "Distributed ledger technology: beyond block chain," *UK Government Office for Science*.

Wright, A., and P. De Filippi (2015): "Decentralized blockchain technology and the rise of lex cryptographia," .

Yermack, D. (2013): "Is Bitcoin a real currency? An economic appraisal," *National Bureau of Economic Research Working Paper*.

A Online Appendix

A.1 What is a Blockchain?

Using blockchain technology, a network of economic agents can agree, at regular intervals, about the true state of shared data. The flexibility in terms of what such shared data represents makes the technology extremely versatile, and allows distributed ledgers to track and settle exchanges across multiple types of digital assets. The rules through which the network reaches consensus about the state of the shared data over time are a key aspect of the market design of a crypto token, as they define the incentives for users and contributors of key resources to the platform. The extent towards which the data in a shared ledger is completely public and associated with pseudonims (as in Bitcoin), [14] or can be strategically shielded for anonymity (as in Zcash) is also a market design choice of a specific token. Similarly, the frequency at which the network reaches consensus and the amount of data recorded in each period of time are features that vary across implementations.

The distributed ledger where the shared data resides is called a 'blockchain' because it typically constitutes a chain of blocks of transaction data (see Figure A-2). Each one of the blocks contains valid transaction records for a specific period of time and their attributes. A key attribute of each transaction (and each block) is its timestamp. Blocks are chained together by incorporating a digital fingerprint of the previous block (a hash) in the current block. Any change in the transaction information contained in a specific block would alter such fingerprint, irreparably breaking the chain of consensus linking that block with all subsequent ones. As a result, one can think of a blockchain not only as a large-scale, distributed database, but also as an immutable audit trail where the 'DNA' of each block is incorporated in all following ones, making it impossible to alter history without being noticed.

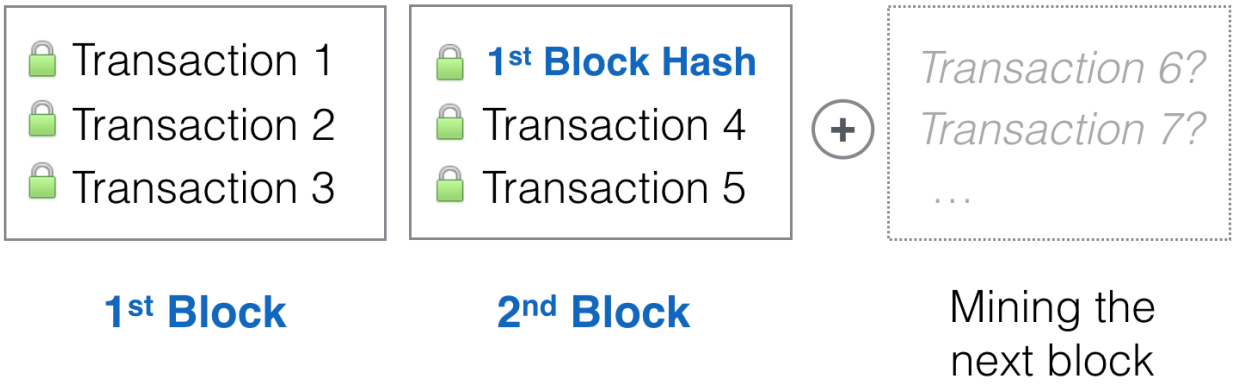

Figure A-2: A Blockchain

[14] Whereas it is often believed that Bitcoin transactions are anonymous, they are actually pseudonymous. Like a writer writing a book under a pseudonym, if a Bitcoin user is ever tied to a specific address, the entire history of her transactions with that address can be read on the public Bitcoin blockchain.

A.2 Proof of Work and 'Mining'

In proof-of-work systems (PoW) such as Bitcoin or Litecoin, participants contribute to broadcasting and verifying transactions while "miners" take on the additional computational work required to assemble new, valid blocks and commit them to the shared ledger. The computationally costly tasks involved in mining essentially constitute a lottery for the right to add the next block to the chain. The more computing power a miner dedicates to mining, the higher the chances of winning the lottery by finding a valid new block first and broadcasting it to the rest of the network. Each time a miner commits a new block to the chain it can assign a predefined amount of the crypto token to itself as a reward (coinbase transaction). This reward, combined with the transactions fees participants may have included in their individual transactions to incentivize miners to prioritize them over others in the construction of the next block, serves as an incentive for miners for the work they perform. To incentivize a decentralized network of miners to contribute resources to secure and operate the network, blockchain protocols typically rely on a native, built-in "token" (in Bitcoin, this is represented by an unspent output on the ledger). This explains why Bitcoin and its blockchain are "joined at the hip":[15] for the network to operate in a decentralized way without trusted intermediaries, the process of maintaining the shared ledger must generate enough of an incentive in bitcoin for attracting miners.

Interestingly, in proof-of-work systems, mining does not serve the purpose of verifying transactions (this activity is fairly light computationally), but of building a credible commitment against an attack: since blocks are chained together, the audit trail formed over time becomes more difficult to tamper with as more blocks are added, and computing power has been sunk to support it. Consensus about the true state of a distributed ledger therefore emerges and becomes stronger as time (and blocks) go by. If a bad actor wanted to reverse a past transaction (e.g. one that is stored n blocks in the past), it would have to spend a disproportionate amount of resources to do so. This is the result of the bad actor not only having to outpace the growth rate of the legitimate chain (which is still maintained by the rest of the network), but also of having to recompute all blocks after the one that is being manipulated. Since the network always takes the longest, valid chain as the true state of the ledger (i.e. as the "consensus"), the task of altering a past block of transactions and imposing it on the rest of the network becomes increasingly difficult as the chain is extended.[16]

As a result, in proof-of-work systems, a blockchain is only as secure as the amount of computing power dedicated to mining it. This generates economies of scale and a positive feedback loop between network effects and security: as more participants use a crypto token, its value increases, which in turn attracts more miners (due to higher rewards), ultimately increasing the security of the shared ledger. Similarly, if confidence in a crypto token drops

[15] See http://avc.com/2015/11/are-bitcoin-and-the-blockchain-joined-at-the-hip/ and http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/ (accessed 11-01-2015).

[16] Ironically, even if bad actors managed to control a disproportionate share of the computing power dedicated to securing a specific blockchain, it would be in their rational best interest to keep mining honestly (and earn the corresponding mining rewards and transaction fees), as tampering would be visible to others and would destroy the value of the underlying cryptocurrency.

(e.g. because of a security flaw or because of conflict between developers on its future direction), its value would drop, possibly triggering a negative feedback cycle where miners leave the ecosystem because of the lower rewards until the point where the ledger becomes insecure and is rendered useless. Whereas proponents of alternative consensus systems (such as proof-of-stake) criticize proof-of-work for being inherently wasteful (e.g. in terms of electricity, hardware), from a game theoretic perspective it is exactly the wasteful nature of the mining computations that defends the ledger from an attack: i.e. the sunk, irreversible commitment to the audit trail constitutes the cost a bad actor would have to sustain to manipulate it.[17]

The process through which consensus on the true state of a distributed ledger is reached and secured over time has implications for market design. Depending on the degree of security needed for a specific transaction (e.g. buying a house versus buying coffee), participants will want to wait for a different number of blocks to be settled after the one containing their transaction. This means that the interval at which a new block is added to the chain and consensus is formed, together with the maximum number of transactions that can be included in a block (block size) endogenously determine the optimal transaction type on a specific blockchain. Whereas participants can include higher transaction fees to entice miners to grant them priority within the first available block (i.e. they can reward miners with a higher transaction fee to increase their priority in the queue of unsettled transactions), there is still a limited number of transactions that can be included in any single block.[18]

From a standards perspective, whereas there are advantages to being able to rely on a single blockchain because of economies of scale in security and direct and indirect network effects, it is clear that a single blockchain will not be able to perfectly accommodate every type of transaction (e.g. exchange of value versus the execution of software applications

[17]If the output of mining was useful for some other purposes too (e.g. if the computations helped find large prime numbers), then the marginal cost of mining would be lower (as part of the cost would be absorbed by the benefits the miner can obtain from selling the solutions to these problems), and the network would be less secure. Proof-of-stake, where the ability to extend a ledger depends on one's ownership stake in the currency, is among the proposed solutions to this trade-off between security and wasteful computations. See: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf and https://bytecoin.org/blog/proof-of-activity-proof-of-burn-proof-of-capacity/ - accessed 09-07-2016.

[18]For example, Bitcoin currently adds a new block every 10 minutes, and blocks currently have a size of 1MB. The alternative cryptocurrency Litecoin was instead designed with shorter confirmation times (2.5 minutes): while this means that less computing work is done for each block (and therefore the sunk commitment and security per block is lower), the shorter time interval between blocks makes Litecoin more suited for smaller transactions. This basic trade-off between security and bandwidth also affects how different stakeholders within an ecosystem view scaling: in the case of Bitcoin, startups and users that see it predominantly as a cheap medium of exchange would rather have it process a large number of transactions per second and keep transaction fees low, whereas others that are interested in security because they see the token as a store of value ('digital gold') would rather have the incentives system drive out smaller transactions to other blockchains through fees and keep the same level of decentralization. Solutions like the Lightning Network enable instantaneous transactions between users through bidirectional payment channels (as in correspondent banking). If successful, this approach would allow a large number of payments to be routed through this parallel network of two-parties ledger entries, drastically reducing the number of transactions that need to be recorded on the main ledger.

or of legal contracts). The size of a transaction, its attributes and functionality, and the related degree of security and privacy needed to execute it will push different marketplaces on different blockchains.[19]

A.3 Permissionless versus Permissioned Blockchains and Privacy of Transactions

Bitcoin's market design choices were driven by a desire to make the cryptocurrency as decentralized and democratic in its governance as possible:[20] there are no trusted intermediaries, anybody can become a miner or add legitimate transactions, and nobody can block other participants' transactions. Whereas this makes Bitcoin extremely resilient to attacks and censorship, it also makes it less efficient, in its current form, than centralized payment networks.[21] Permissioned blockchains, which are distributed ledgers where participants typically need to be granted permission to add (or even view) transactions, can instead deliver higher bandwidth because they do not need to rely on proof-of-work for maintaining a shared ledger. When mining is completely absent from a private blockchain, the audit trail is not protected by sunk computational work, and if the trusted nodes are compromised (or if they collude to rewrite the ledger), the integrity of the chain is at risk.[22]

Private blockchains are therefore very similar to the replicated, distributed databases already extensively used by corporations. The introduction of distributed ledger technology in this context is usually motivated by incentives to further standardize operations and increase compatibility across industry participants without, at the same time, changing the pre-existing market structure. It is important to note that while private blockchains benefit from costless verification, they do not take advantage of the reduction in the cost of networking, since control over transactions and assets is still in the hands of trusted nodes. Reliance on trusted intermediaries also comes with advantages, as these systems are more likely to be compatible from the start with pre-existing regulation.[23] Whereas this makes a distributed ledger more compatible with legacy systems, it also ties it back to traditional

[19]Solutions such as sidechains are being developed through which different blockchains could sync and exchange information seamlessly: e.g. daily microtransactions could take place on a sidechain with lower security but faster confirmation times, and end-of-the-day settlement takes place on the Bitcoin blockchain.

[20]Whereas Bitcoin was designed to be fully decentralized (one cpu, one vote in the consensus process), economies of scale in mining have driven this activity towards centralization. In 2014, one single mining pool reached more than 50% of the network raising concerns about the integrity of the consensus process (as a miner with such a share could potentially censor transactions, revert them or perform double spending).

[21]According to a 2014 stress test, the VISA network was able to handle at peak 56,582 transactions messages per second. As of this writing, Bitcoin can only handle approximately 7 transactions per second (source: http://visatechmatters.tumblr.com/post/108952718025/56582-transaction-messages-per-second and https://en.bitcoin.it/wiki/Scalability - accessed 09-08-2016).

[22]This makes them less suited for problems where the integrity of the audit trail is paramount (e.g. for regulatory compliance, a network of banks should not be able to collude and revert the state of a distributed ledger ex-post).

[23]For example, they can be designed to allow for ex-post editing of transactions through fiat, a feature that would undermine the very premise of a public, immutable blockchain, but that clearly has value for certain types of financial transactions.

intermediaries as sources of trust. As a result, such a blockchain is unlikely to have a drastic effect on market structure and innovation in the long run.

Related to the issue of trusted intermediaries, is the question of how much privacy a particular blockchain needs to deliver to its users: patterns in a publicly available, distributed ledger can be used to de-anonymize transacting entities behind a pseudonym and gather useful information about the market (Athey, Parashkevov, Sarukkai, and Xia 2016, Athey, Catalini, and Tucker 2017, Catalini and Tucker 2017). To protect their privacy, users can adopt privacy enhancing techniques (e.g. use a new address for each transaction, obfuscate their transactions by mixing them with others), use a truly anonymous cryptocurrency (e.g. Zcash), rely on an intermediary (e.g. a digital wallet provider),[24] or use a system that separates basic information about a transaction (e.g. its existence and timestamp) from more sensitive attributes. Additional, sensitive information could be stored on a private blockchain (or database) and immutably linked to the public blockchain entry using a digital fingerprint.[25] This would preserve the blockchain role as a time-stamping machine, since any tampering with the private record would irreparably break the cryptographic link between the two data sources.[26]

While this is still an active area of research, new protocols are being developed to obfuscate transaction data, offer full anonymity to users through zero-knowledge cryptography, and implement different degrees of access to transaction information. Although perfect obfuscation might be not always possible to achieve,[27] it is clear that different cryptocurrencies will be able to compete also in terms of the privacy level they provide to their users (either at the protocol level, or through a trusted intermediary).

As discussed in the paper, costless verification can take place at the level of a single piece of information. When combined with privacy-enhancing measures, this can solve the trade-off between users' desire for customized product experiences (e.g. when using a virtual assistant like Siri), and the need to protect their private information (e.g. the queries sent to the service). If the sensitive data is stored on a blockchain, users can retain control of their data and license it out as needed over time (e.g. Electronic Medical Records, etc).

[24]Some digital wallet providers do not settle each transaction of their customers on a public blockchain, but only record aggregate inputs and outputs among all their users at regular intervals. These "off-chain" transactions offer a greater degree of privacy from the public, although all information is of course available to the digital wallet provider.

[25]For example, this could be achieved by applying a cryptographic hash function to the private part of the record and recording the output (typically a short string of characters) on the distributed ledger.

[26]The blockchain entry would only act as "proof-of-existence" of the original transaction, and if the private record was lost or destroyed there would be no way from the public ledger to extract that information again.

[27]See https://www.iacr.org/archive/crypto2001/21390001.pdf (accessed 08-01-2016).

A.4 Types of Transactions Enabled By Blockchain Technology

A.4.1 From Atomic Transactions and Immutable Audit Trails to the Exchange of Intellectual Property and Other Types of Digital Assets

An atomic transaction is a transaction that can be fully executed and enforced through a distributed ledger, and whose key attributes can also be verified through the same ledger at a very low cost without the need for an intermediary. Examples include transactions that imply an exchange of cryptocurrency between a buyer and a seller (e.g. a Bitcoin lending contract, a gambling contract) or an exchange between different crypto tokens.[28]

If all we care about proving with certainty is if (existence) or when (timing) a certain transaction took place, then we can use a pre-existing blockchain to do so: e.g. we could rely on the Bitcoin blockchain to prove that we knew a certain piece of information at a specific point in time (proof of existence). Whereas we would not be able to directly embed the information on the Bitcoin blockchain, we could incorporate a digital fingerprint of it (e.g. a hash) inside a regular transaction. The digital fingerprint would then be secured by the proof-of-work done to maintain and extend the Bitcoin blockchain. At the verification stage, we could point the public to our transaction while at the same time revealing our private piece of information (e.g. the lab notes we wanted to timestamp) to prove the immutable link between the two. Without any additional infrastructure, a blockchain allows us to implement a "first to file" system based on a secure, historical record of timestamped, digital fingerprints.

Because of the ability to implement atomic transactions, build immutable audit trails, and simplify settlement and reconciliation across organizations, blockchain technology has seen fast adoption and experimentation within finance and accounting. Within these fields, the technology can be used to create more open, flexible and programmable exchange platforms, substantially extending the concept of double-entry bookkeeping (e.g. examples include Chain, Digital Asset Holdings, Blockstreatm etc.).[29] Beyond time, labor and cost savings, the development of more interoperable exchange platforms for digital assets substantially reduces entry cost for new players in these heavily regulated markets.

Applications also include novel forms of intellectual property registration and content licensing (e.g. Mediachain). Royalties for the use and remixing of IP or digital content can be tracked in a granular and transparent way on a blockchain by all market participants, which is likely to be particularly useful when different parties have conflicting incentives (e.g. in a principal-agent relationship).[30] Pricing and digital privacy models are also becoming

[28] Online gambling is an interesting example because costless verification allows for the house to transparently demonstrate fair odds, as users can ex-post verify a dice roll or deck reshuffle was not manipulated to favor the house. Reputation of the gambling house would still be important, as a one-time defection would only be visible ex-post.

[29] For example, the underlying structure and performance of mortgage-backed security can tracked on a blockchain and made accessible to relevant parties in real time (including regulators), and accounting records can be audited in an automatic fashion while preserving the privacy of the entities involved.

[30] For example, artists that license their music to Apple or Spotify could track how many times their songs are played by consumers, or seamlessly receive royalties from other artists for remixes that include parts

more flexible and granular thanks to crypto tokens: e.g. with micro-payments implemented within a browser (e.g. Brave), users can seamlessly pay for access to content behind a paywall, or for an ad-free or no-tracking experience. Similarly, content creators and advertisers can reward users for their attention or for revealing their preferences (e.g. BAT).

A useful extension of an atomic transaction is one that relies on an external source of information (e.g. weather data, exchange rate, price of a stock, outcome of public events) to execute a contract. Examples range from prediction markets (e.g. Gnosis) to betting denominated in a crypto token, to future contracts, mining pool contracts, escrow contracts etc. The external source of information (an 'oracle') could be a trusted intermediary, the aggregation of multiple sources (to avoid manipulation), a crowdsourced voting mechanism, or a trusted hardware device. A particularly interesting set of transactions is the one enabled by linking an IoT device to a cryptocurrency. If the hardware device is secure and cannot be tampered with, then the information it collects can act as the trusted arbiter in a digital transaction.[31] This allows new marketplaces to emerge where energy (e.g. from solar panels), bandwidth, access to resources and information, data processing through an API, or work performed by the crowd are priced in novel ways.[33]

A.4.2 The Identity, Credentials and Provenance Verification Problem

The process of identity verification is central to all economic transactions. Each time we authenticate ourselves (or an entity we represent, or a device), we are essentially creating a transaction allowing a third-party to verify that we are authorized to perform an action. This transaction is usually what stands between a legitimate use and fraud, leakage of information, digital and physical theft. A well functioning market (and economy), relies on robust identity verification as well as on the ability to verify the goods and services being exchanged (e.g. in terms of their provenance, how they were changed through the supply chain etc.), and the credentials of the parties involved (e.g. degrees on a curriculum vitae, professional licensing status, bad actor status, driving record etc.). Current solutions to the identity and credentials verification problem typically rely on insecure secrets and documents (e.g. social

of their songs according to a predetermined smart contract. Similarly, backers on a crowdfunding platform could obtain royalties each time a song they funded is played, artists could sell the rights to the first copy of a digital artwork, stock photography websites could certify legitimate uses of their content at a lower cost.

[31] For example, a weather or pollution sensor[32] could capture local information and sell it back to the network for a price. IoT devices and robots, when combined with a cryptocurrency, can seamlessly earn, barter or exchange resources with other devices on the same network. In a futuristic scenario, a self-driving car could buy up lane space from surrounding vehicles on a highway for priority. If the IoT device also contributes to mining the underlying cryptocurrency (e.g. by dedicating computing cycles during idle time to securing a digital ledger), then this may also allow for new business models to emerge (e.g. a cellular phone's plan could be partially subsidized through its mining chip).

[33] Given current technology, users can already be paid instantaneously and with less frictions through a cryptocurrency to perform small tasks both offline and online across the globe (e.g. answering surveys, translating text or audio, writing a review, training machine learning algorithms, collecting offline prices etc.). Whereas payments from users to services online are pervasive, the reverse flow is substantially more rare (e.g. Amazon Mechanical Turk) and cumbersome (e.g. linking of a bank account). Crypto tokens, by enabling bidirectional, low friction exchange of value, can substantially expand these markets (e.g. 21.co).

security number, passwords, passports, signatures, university transcripts etc.) or public-key encryption and hardware (e.g. multiple factor authentication, certificates). In many cases the intermediary is the government, although it can also be a consortium, or a private firm (e.g. Facebook Connect). This always involves some degree of information leakage and risk of reuse of private information outside of the designated transactions. Blockchain technology can reduce this risk by allowing for authentication without disclosure of sensitive information. The same way a distributed ledger can track the attributes of financial transactions, it can also track changes to an individual's status and credentials (or firm, good, service). An individual's ability to perform (or not) a certain action could be tracked on a blockchain and queried when needed without necessarily disclosing all underlying information (e.g. a bank could verify, after being authorized by a customer, a credit history). Similarly, access to medical records could be granted, revoked or ported between providers as needed.

From a privacy perspective, the ability to license out subsets of personal information for limited amounts of time and to seamlessly revoke access when necessary has the potential to not only increase security, but also to enable new business models where customers retain greater control over their data and firms can dynamically bid for access.

Attributes of digital and physical goods can also be tracked on a distributed ledger as they move through the economy, increasing our ability to verify their integrity, provenance, manipulation and status (e.g. warranties, food safety) over time. This is particularly powerful when immutable properties of a good (e.g. the properties of a diamond, art piece or geographic coordinates of a parcel of land) can be reliably recorded on a blockchain, i.e. when a unique, digital fingerprint can link ownership of a blockchain token to the underlying asset. When this is not possible, the problem of identity, credential and provenance verification will still require trusted intermediaries (or at least a secure IoT device or sensor) to reliably capture what is happening in the offline world and record it on a distributed ledger: Intermediaries and secure devices act as key complements to online forms of verification enabled by blockchain technology.

A.4.3 Online Reputation Systems

A key function of online intermediaries is to design and maintain a robust reputation system to facilitate transactions between buyers and sellers (Luca 2017). In this context, blockchain technology can be used to increase transparency, ensure that reviews and ratings are only produced after a verified purchase, and to build open reputation platforms. Advantages include the ability to port and use the resulting reputation scores across different services and contexts, increased transparency, and lower barriers to entry in markets currently dominated by a few intermediaries (e.g. Yelp, Airbnb, Uber). This has implications for how policymakers approach regulation, monitoring, and antitrust issues in these markets, as it gives a public entity the ability to enforce market design rules (e.g. safety standards, worker compensation, liquidity standards etc.) through a well-designed protocol.

A.4.4 Central Bank Money

A particularly interesting application is the development of a blockchain-based, fiat-endorsed digital currency. If a central bank were to switch from the current infrastructure to a cryptocurrency, it would be able to directly provide citizens with digital, central bank money. This would challenge some of the revenue models of commercial banks, as citizens may prefer the more secure central bank money to their traditional checking account. Startups could then compete in providing security and protection for consumer digital wallets, payments and billing services, etc. While the implications of such a switch are not the focus of this paper, the change would have broad implications for how governments implement taxation (because of costless verification), manage money supply and interest rates, deliver quantitative easing, on their ability to enforce financial sanctions on other governments, and more generally facilitate intertemporal transactions in the economy. Such a currency would also become an appealing alternative - because of its digital nature - for foreign citizens in countries facing currency devaluation or where trust in the government is low. Events such as India's demonetization of the 500 and 1000 rupee notes, and broader pushes towards greater traceability and government surveillance in transactions (e.g. by reducing the role of cash), are likely to increase consumers' interest in cryptocurrencies as a store of value and for privacy concerns (i.e. fiat-based currencies will have to increasingly compete with their decentralized counterparts). Recent moves such as the Chinese ban of initial coin offerings and Bitcoin exchanges foreshadow increasing tension between regulators and permissionless cryptocurrencies, possibly while the same governments consider adopting blockchain technology to lower cost and enable new types of services for their citizens through a fiat-based digital currency.

A.4.5 Auctions

Economists have made great strides in applying economic theory to the design of practical markets (Roth 2002). But issues remain and, apart from once-off auctions of public assets, the best designs are not often implemented. An example of this is the second-price auction developed by William Vickery (Ausubel, Milgrom, et al. 2006), where bidders submit their reservation price to an auctioneer, and the bidder with the highest bid wins the auction but only has to pay the second highest bid. This auction has the property that its outcomes are efficient (the auction winner is the agent with the highest valuation), and involves a straightforward bidding process since bidders can simply submit the highest amount they would be willing to pay. Nonetheless, it has found limited applicability in practice. A notable exception is Google's AdWords auction (Edelman, Ostrovsky, and Schwarz 2007). One of the reasons why market designs that require agents to submit their true valuation (or costs) do not actually emerge in practice is that there is a potential lack of trust in the intermediaries involved. One aspect of this is that a seller may use the fact that a bidder has a high willingness to pay for an object to somehow turn the tables on them in the auction.[34]

[34]For example, suppose there are two bidders for an object. One has a value of $5 and another has a value of $10. Suppose also that it turns out that the seller will keep the object if it does not attract more

Hence, they may choose not to do so and the value of the auction may be undermined. An open-cry auction may resolve this issue by forcing the seller to reveal when their reserve price is met but such auctions have their own costs (including having to assemble all bidders at the same time and location) and may not be practical online.

A distributed ledger solves these potential expropriation problems. For instance, eBay offers an automated bidder which allows people to submit their highest bid and then bids on their behalf. In effect, it is supposed to replicate a second-price auction. Often people do not actually use the automated bidder properly and wait until the last minute to bid (Roth and Ockenfels 2002). One reason could be some kind of mistrust or alternatively a concern that the bids will not be submitted properly. With a distributed ledger, the bids could be collected through a smart contract without ever exposing the information to the seller or a third party. When the auction closes, the contract would rank the offers, identify the winner, and destroy the information about the other bids. The smart contract could also ensure that the bidder has enough funds to make an offer and does not default (Milgrom 2004), reducing the worry that the auction will be re-run and the bidding information used against participants. Thus, we can see how the full verifiability that accompanies a blockchain can potentially render practical the full commitment assumptions required for efficient auction designs to be implemented.

than \$4 in the auction. In a second-price, auction where bidders bid their true values, the winning bidder would be the \$10 value bidder who would only have to pay a price of \$5. Suppose, however, that the seller does not reveal their reservation price. A concern might arise that they might see the bids and then claim the reservation price is \$7. In that situation, the bidders would face expropriation and a reduced surplus from bidding their true values. See (Rothkopf, Teisberg, and Kahn 1990) for an analysis. The authors also examine what might happen if truthful bids leak to third parties who can then exploit the bidders.