Some Simple Economics of the Blockchain

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

November 23, 2016

Abstract

We rely on economic theory to discuss how blockchain technology and cryptocurrencies will influence the rate and direction of innovation. We identify two key costs that are affected by distributed ledger technology: 1) the cost of verification; and 2) the cost of networking. 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 at multiple points in time. Blockchain technology, by allowing market participants to perform costless verification, lowers the costs of auditing transaction information, and allows new marketplaces to emerge. Furthermore, when a distributed ledger is combined with a native cryptographic token (as in Bitcoin), marketplaces can be bootstrapped without the need of traditional trusted intermediaries, lowering the cost of networking. This challenges existing revenue models and incumbents's market power, and opens opportunities for novel approaches to regulation, auctions and the provision of public goods, software, identity and reputation systems.

Keywords: blockchain, cryptocurrency, Bitcoin, distributed ledger technology, market design.

*Christian Catalini is the Fred Kayne (1960) Career Development Professor of Entrepreneurship, and 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 and Catherine Tucker for helpful discussions. Download the most recent version of this paper at http://blockchain.mit.edu

1 Introduction

In October 2008, a few weeks after the Emergency Economic Stabilization Act rescued the U.S. financial system from collapse, Satoshi Nakamoto 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, the internet was about to experience the effects of a drastic reduction in two related costs: 1) the cost of verification; and 2) the cost of networking.[1] For the first time in history value could be reliably transferred between two distant, untrusting parties without the need of a costly intermediary.

Through a clever combination of cryptography and incentives, the blockchain - the distributed public ledger recording every bitcoin transaction - could be used by any participant in the network to query and verify the state of a particular transaction in the digital currency. Thanks to market rules designed to incentivize the propagation of new, legitimate transactions, to reconcile conflicting information, and to ultimately reach consensus at regular intervals about the true state of the ledger in an environment where not all participating nodes can be trusted (e.g. as during a malicious attack to the network), Bitcoin was the first example, at scale, of costless verification. It was also the first example of how a secure network could be bootstrapped without investments by a selected set of 'network operators', but by relying instead on the individual incentives of every participant in the network. As of November 2016, with a market capitalization of approximately $12B, Bitcoin was not only the most diffused[2] and secure[3] cryptocurrency, but also an example of how, as the cost of verification and networking drop dramatically, new types of transactions, intermediation and business models become available.

Because of how it provides incentives for maintaining a ledger in a fully decentralized way,

[1] Whereas the cost of implementing a centralized network has drastically fallen with the internet, the cost of running a distributed, decentralized network was still high before the introduction of blockchain technology.

[2] The market capitalization is calculated as the number of tokens in circulation (approximately 16M bitcoin) times the value of each token (the Bitcoin to USD exchange rate was $740). The second largest cryptocurrency, Ethereum, had less than $1B market cap (source: https://coinmarketcap.com/ - accessed 09-04-2016).

[3] 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").

Bitcoin is also the first example of how an open protocol can be used to implement a marketplace without the need of a central actor. Furthermore, as the core protocol is extended (e.g. by adding the ability to store documents through a distributed file-storage system[4]), as we will see the market enabled by a cryptocurrency becomes a flexible, permissionless development platform for novel applications.

In this paper, we rely on economic theory to explain how costless verification and lower networking costs change the types of transactions that can be supported in the economy, and to identify the types of problems blockchain technology (also known as distributed ledger technology) is likely to have an impact on versus not. Whereas the utopian view has argued that blockchain technology will affect every market by reducing the need for intermediation, we argue that it is more likely to change the scope of intermediation both on the intensive margin of transactions (e.g., by reducing costs and possibly influencing market structure) as well as on the extensive one (e.g., by allowing for new types of marketplaces). Furthermore, for the technology to have any impact in a specific market, verification of transaction attributes (e.g., status of a payment, identity of the agents involved etc.) by contracting third-parties needs to be currently expensive; or network operators must be enjoying uncompetitive rents from their position as trusted nodes above and beyond their added value in terms of market design.

The paper proceeds as follows: in the next Section, we discuss the economics of costless verification and the related reduction in networking costs. In Section 3, we discuss how different market design choices in the development of a blockchain application change its economics. In section 4 we use our theoretical framework to present different applications of blockchain technology. Section 5 concludes.

2 Costless Verification and the Reduction in Networking Costs

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. For example, when an exchange takes place in person the buyer can usually directly assess the

[4]See https://ipfs.io/ (accessed, 9-26-2016).

quality of the goods, and the seller can verify the authenticity of the cash. The only intermediary involved in this simple scenario is the central bank issuing and backing the fiat-currency used in the exchange. If the buyer instead uses a digital form of payment, one or more financial intermediaries broker the transaction by first verifying that the required funds are actually available[5], and then by transferring them to the seller's account. In exchange for their verification services, intermediaries typically charge a fee. The cost of intermediation is one of the transaction costs buyers and sellers incur when they cannot efficiently verify all the relevant attributes of a specific transaction by themselves.

The need for intermediation increases as markets scale in size and reach both geographically and in terms of the number of participants involved. As verification costs increase, markets also become increasingly thin, as fewer buyers and sellers find it profitable to transact. When the cost of successfully verifying the relevant attributes of a transaction outweighs the benefits from the exchange, the market falls apart. The presence of asymmetric information between the seller and the buyer (as in the case where the buyer is unable to assess the true quality or provenance of the goods), is one of these cases. When the market also involves a principal-agent relationship (e.g. as in the case of subprime loans), moral hazard may also lead to unraveling. Common solutions to these problems involve relying on an intermediary for third-party verification, to maintain a reputation system, to force additional disclosures[6] on the seller, to enforce contract clauses designed to generate a separating equilibrium (e.g. warranties), and to perform monitoring.

Interestingly, many of these market design solutions not only require a third-party, but also some degree of information disclosure. This additional leakage of information may constitute a privacy risk for the parties involved, as the data might be reused in the future outside of the original transaction. Classic examples are theft of social security numbers or credit card data. Imperfections in information can also be actively exploited by market participants to establish market power (Edlin and Stiglitz, 1995; Stiglitz, 2001): e.g. banks offering extremely low interest rates on regular savings accounts, but then charging high rates on credit cards.[7]

[5] In some cases, the intermediary also allows the buyer to reverse a transaction if certain conditions are met (e.g. as in the case of a chargeback).

[6] These disclosures will also need to be verifiable to be credible.

[7] Furthermore, they are more likely to offer cards with back-loaded fees to less-educated customers (Ru and Schoar,

As the cost of verification has fallen through history, transactions have become more efficient and new intermediaries and markets have emerged, increasing market thickness and safety. Digitization, in particular, has pushed verification costs for many types of transactions close to zero. Blockchain technology has the potential to complete this process by allowing for the first time for distributed, costless verification. Whereas a distributed ledger allows participants to store and retrieve key transaction information, a secure communication layer is needed to transact using it in the first place: i.e. for costless verification to take place, a secure network needs to exist.

On the internet, transactions have been typically secured on top of open protocols by relying on trusted nodes and intermediaries (e.g. for the provision and validation of certificates, digital payments etc.). With blockchain instead the internet can also act as a secure conduit between untrusted third-parties, as a cryptocurrency protocol itself can contain the rules and incentives for: 1) running a decentralized network; 2) securing a shared ledger at the same time. Under this scenario transaction attributes are stored on a blockchain, and the market design of the underlying cryptocurrency defines how and by whom those attributes can be updated, verified and reused at a future date. Without assigning additional rights to any particular node on the network (e.g. for separating legitimate from illegitimate nodes), a cryptocurrency can create a marketplace without the need for traditional intermediaries. For example, Bitcoin can mimic the core functionality of the SWIFT or ACH financial networks without using banks or vetted institutions as trusted nodes.

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 time it was created, information about the seller and buyer[8] involved in it (i.e. where do the inputs come from, and where should the outputs be delivered), and the fact that it exists at all. Right after the transaction attributes are generated, we typically start relying on them to perform related actions (e.g., once funds are transferred, the seller may ship the goods). Some of these actions take place for every transaction (e.g. settlement), whereas others are only triggered by future events. A particularly interesting subset of future events are those that require additional verification. For example, a problem with

2016).

[8]In this context, as we will see in Section 4, transaction, buyer and seller should be defined in the broadest way possible.

the transaction may emerge, and original attributes will need to be checked again through an audit. The audit is often costly, as it may require a third-party to mediate between buyer and seller. Ideally, the outcome of the audit is the resolution of the problem that just emerged.

Blockchain technology fundamentally changes this flow by allowing, when a problem emerges, for costless verification of all the attributes that can be stored effectively on a distributed ledger (e.g. timestamp of a transaction, other parameters of the original contract, but also, as we will see, digital "fingerprints" of the individuals, goods or services involved). If we think of the audit capability of the third-party (e.g. intermediary or government) that intervenes when a problem emerges in a traditional market as surveillance (or monitoring), blockchain technology can deliver "sousveillance" (Mann et al., 2015), i.e. an audit that is embedded within the marketplace itself. The ability to perform an audit at zero cost through a blockchain is what enables distributed, costless verification.

An additional, key feature of costless verification is that the rules of the audit can be decided ex-ante, reducing the risk of a conflict of interest arising ex-post between the entity in charge of the audit and either side of the market. Furthermore, as we will see in Section 4, privacy enhancing features of blockchain technology can be incorporated in the protocol to avoid leakage of additional information during the audit. Only the parties originally authorized to read the relevant attributes will have access to the information, reducing the privacy risk. Buyer and seller can also agree ex-ante to automate the conflict resolution process through software (and delegate to a third-party oracle[9] when necessary), or make irreversible, credible commitments (e.g. post a bond) without the need for an intermediary.

Taken together, these features of blockchain technology will allow for the unbundling of verification services, as some of the tasks can now be performed at zero cost through a well designed software protocol. Whereas intermediaries will still be needed for handling edge cases (e.g. enforcement of an escrow contract when the goods are of lower quality than expected), many transaction and verification steps can be commoditized. For tasks that can be embedded on a blockchain,

[9]In computer science, an oracle is a Turing machine able to provide, when queried, a solution to a decision problem. For example, if buyers and sellers agreed to different transaction terms based on the weather conditions at a future date, an oracle could aggregate information from multiple weather channels (not controlled by either the buyer or the seller) to adjudicate a dispute.

verification goes from being costly, scarce and prone to abuse, to being cheap and reliable (as the security and integrity of the blockchain guarantees the integrity of the transaction attributes). As the price of verification plummets for these tasks, existing applications will become cheaper (intensive margin effect) and, where optimal, will consume additional verification. New markets will emerge too, as it is now profitable to transact within them because of costless verification (extensive margin effect).

Overall, these changes in the cost of verification and networking also impact the relative cost of using the price system (i.e. a market) over a vertically integrated structure, and the cost of establishing, transferring and maintaining property rights, reputation systems and information markets.

A particularly interesting dimension in this respect is the level at which intellectual property rights can be defined and, relatedly, the level at which the integrity of a piece of information can be assessed. As the cost of verification reaches zero, bits of information that were previously uneconomical to trade on their own, can now be individually verified and possibly become part of how the marketplace operates. 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 piece of information is likely to fundamentally change how information markets are designed. On a blockchain, it is cheap to verify the integrity of an individual transaction or its attributes, i.e. not only a single piece of information can be audited in real time, but its integrity is available to any participant in the network. As a result, verification can be economically implemented at a substantially more fine-grained level than before. For example, accounting information can be built up, with integrity, from the most simple units of transactions, making it substantially more costly to alter a ledger (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.

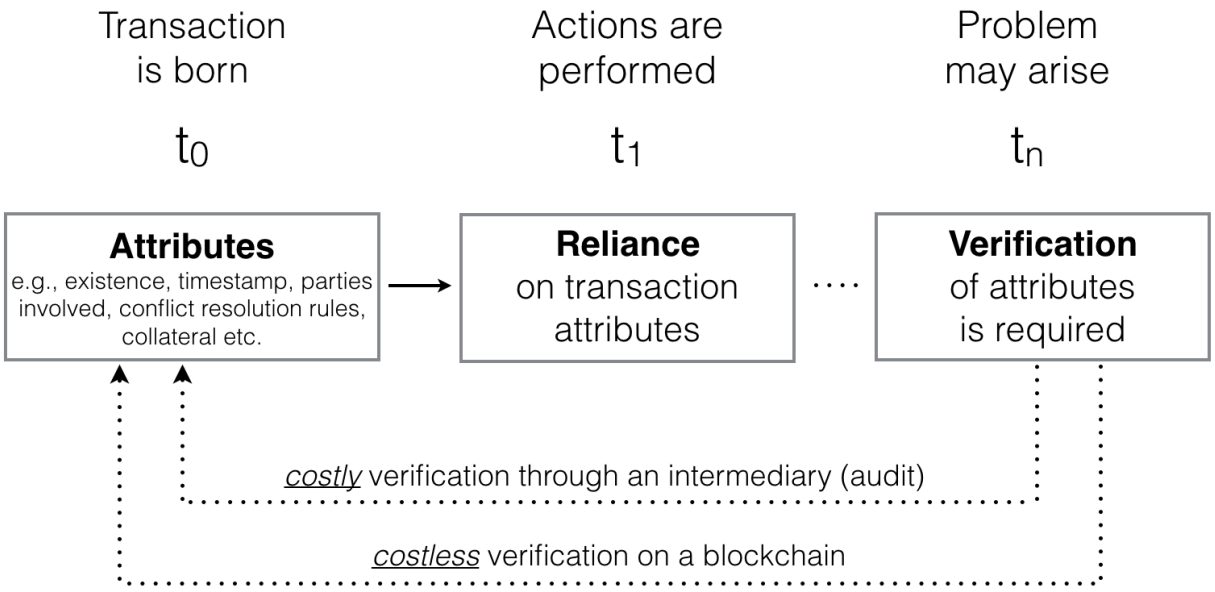

Figure 1: Costly Verification Through an Intermediary (Audit) versus Costless Verification on a Blockchain

3 Market Design and the Blockchain

Blockchain technology has key features of a general purpose technology (GPT). GPTs typically lead to subsequent innovation and productivity gains across multiple industry verticals, sustaining new technological paradigms and economic growth for multiple years (Bresnahan and Trajtenberg, 1995; Elhanan Helpman, 1998; Rosenberg and Trajtenberg, 2001; Moser and Nicholas, 2004). Classic examples of general purpose technologies include the steam engine, electricity, the internet. Because of the inability of a single firm to appropriate all the benefits generated by a GPT (positive externality), underinvestment may occur.

Whereas there are many different types of distributed ledgers being currently developed, for the purpose of this paper we abstract away from these idiosyncratic, often competing implementations and focus on the high-level features that have implications for market design.[10]

As the term suggests, a blockchain is fundamentally a chain of blocks (see Figure 2). Each one of these blocks contains a set of transaction records and their attributes. A key attribute

[10]As a result, we simplify many of the technical constructs. For a detailed description of blockchain technology and Bitcoin, see Narayanan et al. (2016), "Bitcoin and Cryptocurrency Technologies". Available at: https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1 (accessed 09-05-2016).

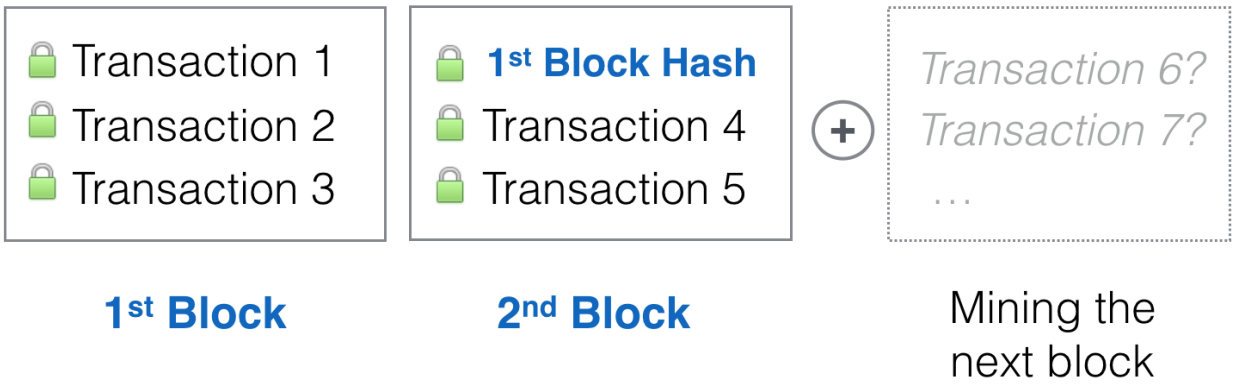

Figure 2: A Blockchain

of each transaction (and each block) is its timestamp: as a result, one can think of a blockchain not only as a giant, distributed ledger, but also as an immutable audit trail. The resulting log of past transactions is typically public (as in Bitcoin or Ethereum), although users can protect their privacy by transacting under multiple pseudonyms[11] (e.g. they can use a bitcoin address for each new transaction), by pooling their transactions with other users to make the traceability of inputs and outputs more difficult,[12] or by using a protocol that offers full anonymity (e.g. Zcash).

3.1 Incentives to Extend and Secure a Distributed Ledger and Implications for the Optimal Type of Transactions

Participants in the network contribute to broadcasting and verifying new transactions, while "miners" take on the additional work of committing new blocks of transactions at regular intervals. In proof-of-work (PoW) systems like Bitcoin, miners perform computationally costly tasks to participate in what essentially constitutes a lottery for the right to add the next block to the chain. Each time a miner commits a new block to the chain it can assign a predefined amount of the cryptocurrency 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 to miners for the

[11] 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.

[12] See https://bitcointalk.org/index.php?topic=279249 (accessed 09-05-2016).

work they perform. The need to incentivize a decentralized network of miners leads blockchain protocols to typically have a native, built-in "token" of some value (in Bitcoin, this is represented by an unspent output on the distributed ledger). This ties the blockchain to the cryptocurrency it is secured by, and explains why Bitcoin and its blockchain are "joined at the hip":[13] for the protocol to work in a decentralized way (i.e., without relying on trusted intermediaries), the process of extending and securing the blockchain itself must generate enough of an incentive for participation (native token).

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: the audit trail build by the addition of subsequent blocks becomes more difficult to tamper with over time as more computing power (and energy) 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.[14] 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.[15]

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 cryptocurrency, the value of the underlying token increases (because the currency becomes more useful), which in turn attracts more miners (due to higher rewards), ultimately increasing the security of the ledger.[16] Whereas

[13] 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).

[14] Since blocks in the chain are cryptographically linked to each other.

[15] Ironically, even if a bad actor managed to control a disproportionate share of the computing power dedicated to securing a specific blockchain, it would be in her 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.

[16] Similarly, if the value of a cryptocurrency drops substantially (e.g. because participants do not believe the

proponents of alternative consensus systems (such as proof-of-stake, proof-of-burn and hybrids) 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 keeps the ledger secure (i.e. the sunk, irreversible commitment to the audit trail).[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 by a specific transaction (e.g. the sale of a house versus the payment for a coffee), participants will want to wait for a different number of blocks to be settled after the one containing their transaction.[18] This means that the interval at which a new block is added to the chain and consensus is formed (which in proof-of-work depends on the difficulty of mining[19]), together with the maximum number of transactions that can be included in a block (i.e. the block size) endogenously determine the optimal transaction size on a specific blockchain. Whereas participants can include higher transaction fees to entice miners to grant them priority within the first available block, there is still a limited number of transactions that can be included in any single block. For example, Bitcoin currently adds a new block every 10 minutes, and blocks currently have a size of 1MB. The alternative cryptocurrency Litecoin[20] was instead designed - among other differences - 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.[21]

underlying protocol is being developed at the right pace or in the right direction), this may trigger a negative feedback cycle, with miners leaving until the point where the distributed ledger is vulnerable to an attack and rendered useless.

[17] If the mining activity was useful for other purposes too, e.g. if the computations helped solve useful computational problems, 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. There is active research to find solutions to avoid this trade-off, including the use of mining for generating a public good (e.g. the discovery of new prime numbers), systems that rely on proof-of-stake (where the ability to extend the blockchain depends on one's ownership stake in the currency), proof-of-activity, and other hybrids. 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] As security increases with the number of subsequent, confirmed blocks, or 'confirmations'.

[19] It is important to note that the difficulty of mining directly relates to the security of the distributed ledger, since it constitutes the amount of computing work required to generate a valid block.

[20] See https://litecoin.info/ - accessed 09-07-2016.

[21] This basic trade-off between security and bandwidth also affects how different stakeholders within the same ecosystem view scaling: in the case of Bitcoin, startups and users that see it predominantly as a cheap payment network would rather have it process a large number of transactions per second and keep transaction fees low, whereas others that are more interested in settlement and larger transactions would rather have the market design

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 and use (e.g. exchange of value versus the execution of a script). The size of a transaction, its attributes and functionality (e.g. Ethereum's comparative advantage in the development of applications and smart contracts using the cryptocurrency), and the related degree of security and privacy needed before fully executing it will push different marketplaces on different blockchains.[22] Whereas each blockchain will be able to provide costless verification, the market design choices made by its developers will define what is likely to be verified on it versus not, and the degree of market power that trusted intermediaries will be able to retain in that specific marketplace.

3.2 Networking Costs, Trusted Intermediaries and Market Structure

Similarly, the design of blockchain technology will depend on how decentralized a market can be versus how much of it functioning will still need to rely on trusted intermediaries (also from a regulation perspective). In the case of Bitcoin, the original choices were driven by the desire to make the cryptocurrency as decentralized as possible:[23] i.e. there are no trusted intermediaries, anybody can become a miner, anybody can add legitimate transactions to the blockchain, nobody can block other participants' transactions from being confirmed and added to the chain. Whereas this makes Bitcoin extremely resilient to attacks and censorship, it also makes it less efficient, in its current form, than a centralized payment network like VISA.[24]

drive out smaller transactions to other blockchains through fees in order to keep the same level of decentralization. Solutions like the Lightning Network (https://lightning.network/) use the native smart contract capability of Bitcoin to enable instant payments between users through bidirectional payment channels. If successful, this approach would allow a large number of payments to be routed through this network of two-parties ledger entries (as in correspondent banking), drastically reducing the number of transactions that need to be committed to the Bitcoin ledger.

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

[23] Whereas the original concept for Bitcoin was for the digital currency 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 double spend).

[24] 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).

Fully private and "permissioned" blockchains, which are distributed ledgers where participants typically need to be granted permission to add (or even view) transactions,[25] 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.[26] 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 full advantage of the reduction in the cost of networking enabled by cryptocurrencies, 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 privacy and compliance requirements. For example, they can be designed to allow for ex-post editing of transactions through fiat[27], a feature that would undermine the very premise of a public, immutable blockchain, but that clearly has value for certain types of financial transactions. Whereas this makes a distributed ledger more compatible with legacy systems, it also ties it back to traditional intermediaries as sources of trust. As a result, such a blockchain is unlikely to have a drastic effect on market structure.

While totally permissionless networks like Bitcoin pose clear challenges in terms of regulatory compliance (e.g. with Anti-Money-Laundering and Know-Your-Customer regulations), do not necessarily integrate with existing business models, and may pose a threat to incumbents, they also offer a more significant opportunity for increasing transparency, competition and innovation in the

[25] In a way that resembles existing financial networks such as ACH or SWIFT. See http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf and http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf (accessed 11-01-2015).

[26] 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).

[27] http://www.nytimes.com/2016/09/10/business/dealbook/downside-of-virtual-currencies-a-ledger-that-cant-be-corrected.html, http://fortune.com/2016/09/20/accenture-blockchain/ (accessed 09-26-2016).

market. On a permissionless blockchain, anyone can build on top of the protocol without worrying about expropriation or censorship by other participants in the network. Permissionless blockchains could therefore be used to increase competition within markets where intermediaries have accumulated a substantial degree of market power because of their custodial and certification services. As ownership of assets (like other transaction attributes) can be easily tracked and managed directly on a distributed ledger, the role some of these gatekeepers play is likely to be substantially reduced if a permissionless blockchain achieves enough diffusion.

To summarize, while costless verification has the potential to increase economies of scale and market power (as it disproportionately lowers costs on the intensive margin of transactions), the reduction in the cost of networking brought by cryptocurrencies could have a counterbalancing effect on competition. When assets are fully digital and ownership over them is not exclusive to a set of trusted intermediaries, new business models can emerge and new entrants can compete for the same market at a lower cost.

3.3 Privacy

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, 2016; Catalini and Tucker, 2016).

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 fully anonymous cryptocurrency (e.g. Zcash), rely on an intermediary (e.g. a digital wallet provider[28]), 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 cryptography.[29]

[28] 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.

[29] For example, this could be achieved by applying a cryptographic hash function to the private part of the record

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.[30]

While this is still an active area of research, new protocols are being developed to obfuscate transaction data[31], offer full anonymity[32] to users, and implement different degrees of access to transaction information. Although perfect obfuscation might be not always possible to achieve,[33] 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 Section 2, 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).

4 Application of Costless Verification

Which applications of blockchain technology are more likely to be developed first? While there is still a high degree of technological uncertainty, development will endogenously evolve based on the markets and types of transactions that are more likely to benefit from the technology first. In the next sections, we rely on economic theory to identify some of them. Issues such as how the technology can scale to thousands of transactions per second (as currently handled by existing financial networks), or how it can deliver different degrees of privacy while still performing costless verification, are likely to be resolved as research and development advances because of specific use cases. As for other general purpose technologies, blockchain is likely to exhibit spillovers across its applications, as breakthrough in one domain (e.g. in terms of security, privacy or other extensions)

and recording the output (typically a short string of characters) on the distributed ledger.

[30]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.

[31]See https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ (accessed 08-01-2016).

[32]Digital currencies like Zcash (ZEC) rely on zero-knowledge cryptography to deliver full anonymity to all participants involved.

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

can be easily ported to others.

Since the costs of using blockchain technology will be relatively high at the beginning (e.g. scarcity of the complementary human capital, learning and adaptation costs), we are more likely to see high value applications that can be implemented on top of existing blockchains, private blockchains targeted at making existing infrastructure more efficient (e.g. in finance and accounting), as well as extensive margin applications that enable new marketplaces. Early market applications are also unlikely to have very high volumes, will rely on simple transaction attributes (e.g. existence, timestamp), can be easily integrated into existing value chains, and will often still rely on an intermediary to complete some of the steps of costless verification. The presence of direct and indirect network effects - while it may constitute an obstacle to adoption when combined with market power - could speed up the diffusion of the technology in markets currently neglected by incumbents. This effect is likely to be stronger if the parties that enter, engage and exit a specific market evolve continuously over time (i.e. in environment with less stability).

Of course, the more versus less competitive nature of pre-existing markets will also affect diffusion, as blockchain is more likely to be a compelling upgrade in settings where the cost of verification is currently high because of legacy regulation or infrastructure. This is likely to influence government regulation across different jurisdictions too, and define where we may see a government-endorsed cryptocurrency first, a cheaper payments system running on a distributed ledger, or experimentation with more complex forms of settlement and reconciliation. Because of how blockchain can be used to enable transactions related to identity (e.g. identity verification and authorization for individuals, firms, goods, software etc.), the technology also lends itself to establishing and maintaining markets for reputation. This is important from a government regulation perspective, as a transparent, distributed ledger can be used to address market failures and monitor market participants at a substantially lower cost (especially when combined with a robust identity infrastructure).

In the following sections, we start from the simplest types of blockchain transactions ("atomic transactions") and build progressively towards more complex applications of the technology to see how they benefit from costless verification and lower networking costs.

4.1 From Atomic Transactions to Markets Enabled by the Internet of Things and Crowdsourcing

The simplest way costless verification can be implemented is through an "atomic transaction". In computer science "[a] transaction is a transformation of state which has the properties of atomicity (all or nothing), durability (effects survive failures) and consistency (a correct transformation)." (Gray, 1981). More broadly, in a database system, atomicity is the property that requires a single logical operation on the database to be either fully executed or not (i.e. its steps are atomic or indivisible). For example, this ensures that the transfer of funds from user A to B is only committed if the funds have been both removed from A and allocated to B.

For the purpose of this paper, we will define as an atomic transaction any transaction that can be fully executed on a blockchain, and whose key attributes required for verification are also accessible through a distributed ledger. This means that the transaction can be executed and verified without the need of an intermediary, i.e. without placing trust in anything else but the state of a distributed ledger. Examples include transactions that only 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 digital currencies.[34]

As digital currency adoption increases (and is regulated), atomic transactions are likely to become increasingly useful and competitive relative to pre-existing solutions that rely on an intermediary or financial network. In settings where intermediaries do not add substantial value to payments (e.g. by handling chargebacks, disputes etc.), blockchain technology can commodify the "payment rails", lower entry barriers and increase competition in the market.

An immediate, 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 fully execute a contract. Examples range from prediction markets to betting denominated in a cryptocurrency, to future contracts, mining pool contracts, escrow contracts etc. The external

[34]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 (or other software exploit) would only be visible ex-post.

source of information (or 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 atomic transactions is the one enabled by linking a hardware device (e.g. an Internet of Things device, a solar panel) to a cryptocurrency. If the hardware device is secure and cannot be tampered with, then the information it collects can act as the trusted oracle in a digital transaction. For example, a weather or pollution sensor[35] could capture local information and sell it back to the network for a price. This is a clear example of how costless verification and low networking cost enable new markets to emerge, possibly introducing new models for the delivery of public goods too. Another example is a car key that can read information from a blockchain and use public-key cryptography to authenticate its user: in such a scenario, the sale of a car in exchange for a cryptocurrency could entirely take place on a blockchain, and ownership and access could be tracked on a distributed ledger. Implementing an escrow transaction in such a context would be trivial, as a smart contract would only update the ownership of the car key if the buyer has escrowed sufficient funds to buy it. Such a key could also lower the cost of a car loan, as access to the vehicle could be tied to the repayment schedule. In this particular case, costless verification would take place every time the user requests access to the vehicle still under the loan agreement.

Internet of Things (IoT) devices and robots, when combined with a cryptocurrency, can seamlessly earn, barter or exchange resources with other devices on the same network. 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).[36]

[35] https://medium.com/@21/sensor21-earn-bitcoin-by-collecting-environmental-data-218a4132ca70 (accessed 09-11-2016).

[36] New cryptocurrencies are also actively being designed to force a greater degree of decentralization (e.g. by selecting computation problems that benefit less from economics of scale). Whereas there are currently economies of scale in mining (which resulted in the current centralization of Bitcoin mining), as Moore's law slows down, decentralized mining may become increasingly competitive: "We think that the next step after pooled datacenter mining is massively distributed and decentralized mining, such that millions of mining chips worldwide each generate a small stream of bitcoin. One of the key reasons we believe this is that bitcoin mining has caught up to Moore's law. [...] This indicates that we may be able to distribute mining chips with CPUs, as a new kind of co-processor - much like GPUs or networking cards added new functionality to complement CPUs." Sources: https://21.co/learn/21-mining/#redecentralizing-bitcoin-with-distributed-mining (accessed 09-12-2016) and http://blogs.wsj.com/digits/2015/05/18/bitcoin-startup-21-unveils-product-plan-embeddable-mining-chips/ (accessed 06-01-2015).

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. In a futuristic scenario, a self-driving car could buy up lane space from surrounding vehicles on a highway for priority. Given current technology, users could already be paid instantaneously to perform small tasks both offline and online (e.g. answering surveys, translating text or audio, writing a review, training machine learning algorithms, collecting offline prices etc.) with substantially less friction. 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). Cryptocurrencies, by enabling bidirectional, low friction flows of payments within browsers (e.g. through a plugin), can substantially expand these markets.

4.2 From Simple Transaction Attributes to Complex Forms of Settlement and Reconciliation

Another way to extend an atomic transaction is to use it together with a different, possibly pre-existing database or platform. This allows a legacy system to rely on a blockchain for time-stamping, for building an immutable audit trail or for settlement and reconciliation across different systems (e.g. separate databases between market participants in an industry).

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 value) inside a regular bitcoin transaction. The digital fingerprint would then be secured by the proof-of-work done to maintain and extend the Bitcoin blockchain (just like any other Bitcoin transaction). At the verification stage, we could point the public (or a trusted intermediary) to our Bitcoin transaction while at the same time revealing our private piece of information (e.g. the lab notes we needed 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.

Applications include novel forms of intellectual property registration and content licensing. 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). 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 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,[37] stock photography websites could certify legitimate uses of their content at a lower cost.

Access to information and digital goods (e.g. financial information, online content, software etc.) can be priced and delivered using a blockchain for payment, authentication and contract enforcement. If a buyer fails to renew payment, cancels or upgrades the underlying contract, access can be seamlessly adjusted as needed. Pricing models can also become more flexible and granular: e.g. micro-payments could be implemented in a browser to reward content creators in exchange for a browsing experience without ads, paywalls could be built on top of a distributed ledger to allow for interoperability across multiple outlets etc. (e.g. users could pay a single subscription and seamlessly navigate between different newspapers).

Whereas the flexibility enabled by a blockchain, if anything, increases the value of curation of digital content, it also increases competition for platforms that bridge content, services and payments between multiple sides of a market (e.g. Airbnb, Uber, Netflix etc). Although platforms also contribute to market design by implementing reputation systems and reviews and by certifying content, many of these features can be implemented in a distributed, verifiable way on top of a blockchain, challenging existing revenue models.

[37] Whereas it is impossible to distinguish the first copy of a digital good from any following one, the ownership of a digital painting could be tracked on a blockchain (in a similar way to the ownership of an unspent output - i.e. a "bitcoin" - is tracked on the Bitcoin blockchain).

The ability of a distributed ledger to be used for settlement and reconciliation across different market participants, will possibly have its first, tangible impact in finance and accounting. In these fields, blockchain technology can be used to create a more open, secure financial platform, substantially extending the concept of double-entry bookkeeping. Costless verification and the reduction in networking costs have implications for competition and regulation in these markets too, as they can commoditize parts of settlement and reconciliation, and allow for novel forms of transparency and monitoring of financial actors. For example, the underlying structure and performance of a mortgage-backed security could be tracked on a blockchain and made accessible to relevant parties in real time (including regulators), or accounting records could be audited in an automatic fashion while preserving the privacy of the entities involved. Beyond time and cost savings, the development of a more interoperable financial platform could substantially lower entry cost for new players in these heavily regulated markets. In finance, multiple startups are trying to challenging existing business models by relying on distributed ledger technology. While blockchain is often used in the backend of these services and is invisible to the consumer, it eventually promises to allow these companies to deliver services at a lower cost than competitors.

4.2.1 Central Bank Money

A particularly interesting example 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, 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. At the same time, 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 currencies like Bitcoin: i.e., in the future fiat-based currencies may have to increasingly compete with their decentralized counterparts.

4.3 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 a certain 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 security number, passwords, passports, signatures, university transcripts etc.) or public-key encryption and hardware (e.g. multiple factor authentication, certificates). In most cases the intermediary is the government, although it can also be consortium, or a private firm (e.g. Facebook Connect). As discussed in Section 3.3, 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). For example, an individual's ability to perform (or not) a certain action could be recorded on a blockchain and queried when needed by a third-party (e.g. a bank could verify, after being authorized by a customer, her status in the country or credit history). Similarly, access

to medical records (or parts of them) 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.

4.4 Reputation Systems and Decentralized Platforms

A key function of online intermediaries is to design and maintain a robust reputation system to facilitate transactions between buyers and sellers (Luca, 2016). In this context, blockchain technology can be used to increase transparency, ensure that reviews and ratings are only produced after a verified purchase, but also to build an open reputation platform. Advantages of the latter include the ability to port and use the resulting reputation scores across different services and contexts, increased transparency, and possibly increased competition 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.

For example, if a cryptocurrency were used to match drivers with consumers looking for a ride, startups such as Uber or Lyft would have to compete for each ride based on current market conditions, user preferences (e.g. level of service), and the quality of their certification services (i.e. background checks on drivers and cars). User and driver lock-in into a proprietary platform would

be reduced, as both sides of the market could dynamically select the broker which provides the most added value at that specific moment in time. Alternatively, a fully decentralized, peer-to-peer car-pooling service could be implemented on a blockchain without the need of an intermediary to match requests.

Whereas full disintermediation is often inefficient as intermediaries can add substantial value to transactions in many of these markets (e.g. through curation, certification etc.), developers are experimenting with more decentralized models that reduce (or eliminate) control by a central platform. Cryptocurrencies and their protocols have been used or proposed for decentralized prediction markets, crowdfunding platforms (Lighthouse), to raise investment capital for cryptocurrency-related applications (Ethereum DAO), for cloud storage (e.g. StorJ, Filecoin), digital rights management (e.g. Open Music Initiative), medical records (e.g. MedRec).

In the next section, we explore how permissionless innovation protocols can reshape market structure and lower the cost of experimentation in the markets they are introduced in.

4.5 Permissionless Innovation Protocols and the Theory of the Firm

When a protocol that can reach consensus about the true state of a shared ledger is combined with strong incentives to keep the network running, participants suddenly have access to decentralized, costless verification. The organizational form enabled by this change is a drastic departure both from the structure of a vertically integrated firm, but also from digital marketplaces and open source communities. Whereas firms rely on fiat and control, digital marketplaces on their ability to avoid disintermediation and offer better brokerage between the two (or more) sides of a market, and open source communities on their ability to elicit contributions towards a shared objective, permissionless innovation protocols can deliver the high-powered incentives and efficiency of a market without resorting to traditional forms of intermediation. The protocol becomes the intermediary and market maker, in the same way the TCP/IP protocol clears internet traffic without syndicating its content. For many applications, a cryptocurrency-based protocol resembles a utility, allowing for experimentation and innovation on the applications stack built on top of it.

A key feature of this ecosystem would be the ability of anyone (hence the permissionless nature)

to develop novel applications and compete with others on top of the protocol, while still benefiting from the network effects and adoption of the underlying cryptocurrency. For example, if one wanted to use the Bitcoin blockchain to timestamp legal documents or property titles, such an application would not require any change to the underlying protocol to be implemented, in a way that resembles how internet services (that we could not have possibly anticipated) were developed on top of TCP/IP as the technology became more pervasive in our lives. The ability to innovate in a decentralized fashion makes blockchain technology a general purpose technology, as entrepreneurial experimentation can take place and be rewarded from anywhere in the economy.

A key issue therefore becomes how to sustain and launch such a protocol. In the case of Bitcoin, multiple years passed before the underlying token had any meaningful value and therefore could attract investment and developers' interest. Incentives for mining, speculation and other early use cases (including illegal marketplaces) bootstrapped the value of the currency, increasing the security of the underlying blockchain along with it. Since the value of the token is based on expectations about its utility in the future, the speed at which a new cryptocurrency can be diffused depends directly on the narrative that is used to introduce it, as well as its comparative advantage in terms of market design over alternatives. Interestingly, whereas crowdfunding so far as relied on online aggregators like Kickstarter or AngelList to select and screen projects (Agrawal et al., 2014), each cryptocurrency can act as its own crowdfunding platform, matching computing time and resources to a shared objective, ethos or vision about the future of technology.

By buying the tokens early, investors are essentially sustaining the growth of the ecosystem around the cryptocurrency. Because of how the token appreciates in value as its usefulness is revealed over time, early adopters have a natural way to monetize their private signal about the future: joining early. This reward system, which resembles some of the features of equity contracts in early-stage entrepreneurship, can be used to attract high quality contributions from top developers and interest by early stage professional investors (e.g. angels and VCs).

Relative to open source projects, which have to rely on donations of time and resources (either directly from the community or from firms interested in the underlying technology), or signalling incentives and career concerns (Lerner, 2002), cryptocurrency protocols can offer direct, monetary

incentives to fund their growth. This could expand the set of individuals interested in participating in an open source project, and in some cases could change how we fund the provision of public goods.

Of course, if individuals are risk averse and the initial investment in research and development is substantial, a permissionless, innovation protocol will only be developed if a firm is able to appropriate its benefits through complementary assets, or if a public effort supports its early development as in the case of the internet (Greenstein, 2015). A permissionless innovation protocol could also be mandated as a result of an antitrust intervention to avoid the monopolization of a market (e.g. to reduce concentration in transportation networks like Uber), and to lower barriers to entry. Public-private partnerships or private consortia could also decide to co-invest in a distributed ledger to increase interoperability within an industry and reduce costs. If the provision of a public good can be tracked on a distributed ledger, then blockchain technology can also be used to incentivize individuals or firms to contribute to it. This can help address market failures and price externalities that are currently too costly to track, and can lower implementation costs for pre-existing policies (e.g. congestion tax, cap and trade etc). From a regulatory perspective, the transparency enabled by the blockchain allows regulators to more closely monitor market participants (and relative transactions) on a regular basis and costlessly verify their digital activity trails.

4.6 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 practice' designs are not often implemented. One example of this is the second-price auction that was developed by William Vickery (see Ausubel and Milgrom, 2006). That auction involves bidders submitting bids where the bids are then ranked by the auctioneer, and the agent 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 generally efficient (the auction winner is the agent who has the highest value) and also that bids are straightforward in that bidders can simply submit as a bid the highest amount

they would be willing to pay in the action. Nonetheless, this auction has found limited applicability in practice. A notable exception is Google's AdWords auctions (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. 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 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.[38] Hence, they may choose not to do so and the value of the auction may be undermined. It is observed that 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. This may not be practical for auctions such as those that occur on platforms like eBay.

A blockchain could resolve 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 be submitted properly. With a blockchain, the bids could be registered and then a protocol could be used to replicate the automated bidding option without ever releasing the bids themselves to the seller or any third party. In effect, the auction could have a date upon which it closed and bids would be submitted by that date on the distributed ledger. Then at that precise second, the auction would

[38] See Rothkopf, Teisberg and Kahn (1990) for an analysis. They also examine what might happen if truthful bids leak to third parties who can then exploit the bidders.

run and the winner and price they paid would be announced.

Indeed, we could go further. One difficulty of running auctions is that bidders may not be able to pay and may default (Milgrom, 2004). This possibility is another reason why bidders may not reveal the truth in their bids; that is, they are worried the auction will be re-run and that information may be used against them. When bids are submitted on a blockchain, they could also provide access to another set of information namely, an account verifying at the precise second the auction is run that the bidders are able to pay. The auction is then executed and the winning bid is automatically transferred into an escrow prior to full settlement. The possibility of default is eliminated as is the residual risk that the auction will not be completed.

Thus, we can see how the full verifiability that accompanies the blockchain can potentially render practical, the full commitment assumptions required for efficient auction designs to be implemented.

5 Conclusion

The paper focuses on two key costs that are affected by the introduction of 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. As more of these attributes can be cheaply recorded (or linked) to distributed, shared ledgers, new types of transactions and marketplaces are likely to emerge. Furthermore, through the use of native cryptocurrency tokens, distributed ledger technology can be used to bootstrap networks of exchange that do not rely on traditional intermediaries. In this context, intermediaries can still add value to transactions by focusing on the market design layer that is not commoditized by the use of a cryptocurrency (e.g. they can provide screening services, monitoring etc.), although they are likely to face increased competition because of the ability to cheaply generate and trade digital assets on a more open platform. This challenges existing revenue models and incumbents' market power, and opens opportunities for novel approaches to regulation and the provision of public goods, software, identity, exchange platforms and reputation systems.

References

[1] Agrawal, A., Catalini, C., Goldfarb, A. (2014) “”Some Simple Economics of Crowdfunding.” Innovation Policy and the Economy 14.1: 63-97. University of Chicago Press.

[2] Athey, S., Catalini, C., Tucker, C. (2016) “The Digital Privacy Paradox: Small Money, Small Costs, Small Talk”, Working Paper, MIT.

[3] Athey, S., Parashkevov, I., Sarukkai, V., Xia, J. (2016) “Bitcoin Pricing, Adoption, and Usage: Theory and Evidence”, SSRN Working Paper No. 2826674.

[4] Ausubel, L. M., Milgrom, P. (2006) “The lovely but lonely Vickrey auction.” Combinatorial auctions 17: 22-26.

[5] Bolton, P., Dewatripont, M. (2005) “Contract Theory”. MIT press.

[6] Catalini, C., Tucker, C. (2016). “Seeding the S-Curve? The Role of Early Adopters in Diffusion.” SSRN Working Paper No. 2822729.

[7] Edelman, B., Ostrovsky, M., Schwarz, M. (2007) “Internet advertising and the generalized second-price auction: Selling billions of dollars worth of keywords.” The American Economic Review 97.1: 242-259.

[8] Gale, D., Hellwig, M. (1985), “Incentive-Compatible Debt Contracts I: The One-Period Problem”, Review of Economic Studies 52, 647-64

[9] Gans, J., Halaburda, H. (2013) “Some Economics of Private Digital Currency.” Bank of Canada Working Paper 2013-38

[10] Gray, J. (1981) “The Transaction Concept: Virtues and Limitations.” Proceedings of the 7th International Conference on Very Large Databases.

[11] Greenstein, S. (2015). “How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network.” Princeton University Press.

[12] Mann, S., Janzen, Mir, A. A., Nickerson, K.. (2015) "Declaration of Veillance (Surveillance is Half-Truth)." In Games Entertainment Media Conference (GEM), 2015 IEEE, pp. 1-2. IEEE.

[13] Milgrom, P. R. (2004) "Putting auction theory to work." Cambridge University Press.

[14] Roth, A. E. (2002) "The economist as engineer: Game theory, experimentation, and computation as tools for design economics." Econometrica 70.4: 1341-1378.

[15] Roth, A. E., Ockenfels, A. (2002). "Last minute bidding and the rules for ending second price auctions: evidence from ebay and amazon auctions on the internet." American economic review 92.4: 1093-1103.

[16] Rothkopf, M. H., Teisberg, T. J., Kahn, E. P.. (1990) "Why are Vickrey auctions rare?" Journal of Political Economy: 94-109.

[17] Townsend, R.M., (1979). "Optimal contracts and competitive markets with costly state verification." Journal of Economic Theory 21(2), 265-293.