Is Blockchain Hype, Revolutionary, or Both? What We Need to Know.

April 2018

Sarah Oh & Scott Wallsten

409 12th Street SW ● Suite 700 ● Washington, DC 20024
Tel: (202) 828-4405 ● Email: info@techpolicyinstitute.org ● www.techpolicyinstitute.org

Is Blockchain Hype, Revolutionary, or Both? What We Need to Know.

Sarah Oh[*] and Scott Wallsten[**]

April 3, 2018

Abstract: Will blockchain technology revolutionize the economy, or is it mostly hype? Blockchain is a decentralized protocol for creating and running distributed ledgers that makes it possible to track assets, from land to music to intellectual property to tomatoes to bitcoins, cryptographically without a centralized controlling authority. In principle, the technology holds out the promise of a reliable, trustworthy way of recording asset ownership and transfers in countries with corrupt or otherwise inefficient institutions. Even in countries with reliable institutions, blockchain may provide a method of recording transfers that are otherwise not valuable enough to track cost-effectively with traditional mechanisms. The potential economic gains are enormous. Yet, the underlying economic and institutional problems are generally harder to solve than simply putting assets on a blockchain. The last step between humans and machines seems to be blockchain's weakest link, where error, corruption, rent-seeking, and other incentives can impede economic efficiency. This essay asks a series of questions about blockchain, implications for institutions and future research. How do we think about gains in economic efficiency from this new technology at the margin? How does the hype for blockchain compare to past new technologies? Is blockchain a response to corruption?

Keywords: Blockchain, transaction costs, institutions, corruption

JEL Classification: D02, D73, E42, O30

[*] Research Fellow, Technology Policy Institute. [**]President and Senior Fellow, Technology Policy Institute. The views expressed here are those of the authors and do not necessarily reflect those of TPI's staff, board of directors, or board of academic advisors. We thank Mary Shirley and Claude Menard for thoughtful comments. Forthcoming in Claude Menard and Mary Shirley (eds.) The Research Agenda in New Institutional Economics. Northampton & Cheltenham: Edward Elgar Pub., 2018 (forthcoming) DOI: 10.4337/9781788112512.

I. Introduction

Economies require that transactions be trusted. A buyer must be certain that the seller truly owns the asset she claims to be selling and that her ownership will be widely recognized so that she may reap its returns. The seller, meanwhile, must be able to verify that he will receive the agreed compensation for transferring ownership of the asset. The lower the cost of such "trusted transactions," including the speed at which they are verified, the more types of transactions that can be conducted and the more efficiently the economy will function.

The promise of blockchain is a leap forward in the ability to engage in trusted transactions regardless of the surrounding institutional environment. Trusted transactions recorded in the blockchain give this new technology its potential to be revolutionary. A leading vendor of blockchain services is quoted as saying, "What the internet did for communications, blockchain will do for trusted transactions."[1] As with many potential revolutionary technologies, the key question is whether it will truly be revolutionary or whether it is hype promoted mostly by those, like leading vendors, with a vested interest.

A blockchain is a digital ledger, recording a series of transactions. More specifically, a blockchain records transactions, contracts, money, and so on in "blocks" of data that are "chained" together to form a complete history of that asset, stored on a network of independent computers ("nodes"). A transaction creates a new block of data that must be verified by "miners" before it can be added as a new block to the chain.[2]

Verification, or validation, is key to the integrity of the blockchain and requires several steps. The process begins when a user enters a new transaction, which is "hashed," or coded,

[1] https://www.ibm.com/blockchain/what-is-blockchain.html

[2] The terms "miners" and "nodes" are often used interchangeably, but "mining" generally refers to the process of verifying transactions while "nodes" refers to the machines that store the blockchain and do the processing.

based on the blockchain's particular protocol. As one technology vendor explains, "each block is identified by a hash, a 256-bit number, created by an algorithm agreed upon by the network. A block contains a header, a reference to the previous block's hash, and a group of transactions. The sequence of linked hashes creates a secure, independent chain."[3] Independent miners solve a mathematical puzzle described in the block's header using the agreed algorithm. If a miner receives the correct answer then it verifies the transaction. Once a sufficient number of miners verifies the transaction the block is added to the blockchain.[4]

Blockchains can do more than add blocks to the chain or transactions to the ledger. Smart contracts can be programmed into the blockchain with simple rules to trigger automatic transactions. Beyond the blockchain, new digital ecosystems have also blossomed around the trusted and decentralized ledgers. Off-chain networks allow parties to exchange assets without recording the transaction on the verified blockchain. These off-chain networks can more rapidly execute transactions, because they do not employ the mining protocols that verify each ledger entry. For example, an off-chain network, such as Coinbase or Ripple, allows parties to buy and sell Bitcoin without making changes to the blockchain ledger. These off-chain networks allow for the exchange of a Bitcoin, for example, with other products or services in a growing digital ecosystem.

Interest in blockchain has soared recently along with interest in these new digital ecosystems. Cryptocurrencies like Bitcoin are the most well-known use of blockchain. But potential applications extend far beyond currencies. Hopeful entrepreneurs, Fortune 500 companies, and even an iced-tea company have argued that blockchain can transform society (or

[3] https://www2.deloitte.com/insights/us/en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html

[4] Botjes (2017) aggregates and explains several descriptions of the verification process. https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3

at least iced tea). Some venture capitalists are making large investments in this technology.[5] At the same time, skeptics consider blockchain to be just a marginal advance in secure databases. Many critics consider blockchain to be useful but not transformative. Some blockchain initiatives have already begun to wind down in the financial sector.[6]

We will not know who is right for years, but in this essay we explore possible uses, research questions, and the types of institutional obstacles that may thwart blockchain. We begin by discussing blockchain's benefits in decentralization and reduced transaction costs and then discuss a major weak link—humans and human institutions.

II. Decentralization and Transition and Transaction Costs

Because authentication of new transactions is decentralized, no single institution can or is even necessary to keep the ledger accurate and up-to-date. Many proponents of blockchain believe this decentralization is a key benefit of blockchain because it creates an opportunity to replace inefficient institutions and centralized government oversight in some areas. But decentralization may not always be a net benefit. As Narayanan, et al. (2016, at p. 282) ask, "Is decentralization a good idea? Is it economically feasible? What are the social consequences of decentralization?" More specifically, to be worthwhile, as with any other improvement, the incremental benefits of decentralization minus the costs of transitioning to a new method must be positive. Otherwise the net present value of moving to blockchain will be negative even if the technology itself is superior to what it would replace. Whether blockchain meets that threshold is likely to differ by

[5] https://www.reuters.com/article/us-blockchain-investment-andreessen/blockchain-project-raises-61-million-from-andreessen-horowitz-u-s-hedge-fund-idUSKBN1FR1IX

[6] https://www.reuters.com/article/us-banks-fintech-blockchain/wall-street-rethinks-blockchain-projects-as-euphoria-meets-reality-idUSKBN1H32GO

both what the blockchain is to record and the existing institutions with which it will compete or complement.

Cryptocurrencies

Cryptocurrencies like Bitcoin are easily the best-known use of blockchain to date. Making cryptocurrency real and tradable is a remarkable feat of technology and institution-building. By incorporating features of money into private digital currencies, such as Facebook Credits, Microsoft Points, or Amazon Coins in 2013, or Litecoin, Bitcoin, or Ethereum in 2018, entrepreneurs have created new ecosystems of digital transactions, settlement, and reconciliation of non-money digital tokens. (Gans and Halaburda, 2013; Catalini and Gans, 2016).

Still, its social value is unclear. Most importantly, cryptocurrencies do not yet appear to offer large improvements over existing currencies. As Joshua Gans has reportedly said, "We already have money. It's called money." We also have trusted electronic ways of transferring money, such as SWIFT or ACH financial networks, payment networks like Visa or MasterCard (Catalini and Gans, 2016), and now newer systems like Venmo, Zelle, and Paypal. Additionally, cryptocurrencies remain technologically inferior to existing currencies in some ways. For example, the Visa network could handle 56,582 transactions per second in 2014, while Bitcoin could verify only 7 transactions per second as of 2016 (*Id*. at 11, n.24). It is arguably for all these reasons that despite their hype, cryptocurrencies have not become widely accepted substitutes for existing currencies.[7]

Cryptocurrencies have, however, proven markedly superior to existing monetary instruments for illegal activity. In particular, their decentralized and cryptographic nature has made it the preferred monetary instrument of hackers and others with nefarious objectives.[8] In

[7] http://www.wired.co.uk/article/bitcoin-scale-future-problems
[8] http://fortune.com/2018/01/31/coincheck-hack-how/

many such cases Bitcoin's benefits to criminals easily surpassed the threshold necessary to make using it worth their while. Bitcoin has made possible completely new sources of revenues for them, such as relatively small hacks of personal computers that can then be unlocked with a small bitcoin payment to the hacker. The profitable uses of cryptocurrencies are often so socially unacceptable that some research has even questioned whether cryptocurrencies are a social waste (Williamson, 2018).

The relevant research questions, we believe, are along two paths. The first is whether cryptocurrencies can help identify and promote economically productive activities that existing regulatory systems make difficult. Some of those might fall into the general category of "illegal because they protect an incumbent interest." Research along this path is likely to entail careful study of actions and proposals by central banks and securities regulators to determine whether the expected benefits of those actions exceed their costs and how the costs and benefits are distributed.

The second path involves the role of cryptocurrencies in the blockchain technology itself. As discussed above, a key component of a blockchain is verifying new transactions. Verification requires solving a mathematical puzzle, which requires energy-intensive computational resources. Miners, therefore, need some incentive to spend those resources to verify the transactions. Such an incentive is conceptually simple when the mining is related to currency transactions—a miner can receive some share of the transaction or be awarded currency for being the first to solve a transaction. But what incentive do miners have to verify blockchain transactions unrelated to cryptocurrencies? To put it differently, is blockchain sustainable if cryptocurrencies are necessary for any blockchain to succeed and cryptocurrencies themselves have no value outside of blockchain verification?

Developing Countries, Poor Institutions, and Corruption

Assuming blockchain retains the incentive for miners to verify transactions, blockchain could yield significant benefits in places with poor institutions, such as many developing countries, since the incremental benefits of the technology need not be as large as when existing systems are strong. Additionally, blockchain could support smart contracts that bypass the need for building competent institutions and are, if not corruption-proof, at least more resilient to corruption.

Some economists say blockchain can be a key to enforcing property rights among the poorest people in developing countries. In principle, blockchain provides a method of tracking who owns what and who sells what to whom without government involvement. In other words, it allows for a functioning system of tracking property rights without concern that an incompetent or corrupt government could alter ownership records to suit its own purposes. With the help of external organizations to enter trustworthy data into a blockchain, these countries can have property ledgers that are less prone to tampering, lost records, or missing information.

Yet, a technologically superior approach does not always win the day. Bad institutions will still exist, and governments and others will not appreciate being disintermediated.[9] Even with blockchain, processes like property transactions would still be subject to state involvement and enforcement (Arruñada, 2018). Furthermore, installing blockchain may prove challenging for weak governments. If the technology is too complicated, then governments may find that old systems are easier for bureaucrats to manage, albeit poorly. In other words, the same factors that keep more standard forms of record-keeping and enforcement from working will also work to

[9] As the inestimable Malcolm Reynolds said on Season 1, Episode 10 of *Firefly*, "…eliminating the middleman is never as simple as it sounds. About 50 percent of the human race is middlemen, and they don't take kindly to being eliminated."

keep blockchain-based methods from succeeding. Whether blockchain can overcome these problems remains to be seen and to be studied.

To begin to answer this question, researchers should study pilot programs that aim to use blockchain to overcome bad institutions. For example, economist Hernando de Soto and Overstock CEO Patrick Byrne began a program to develop property registries in developing countries using blockchain. By one report, this initiative modestly "aims to create a global property registry blockchain as a utility that will unlock dead capital, help five billion people have modernized property rights, give information necessary to settle property conflicts/disputes and to fight terrorism by undermining terrorists' business model."[10] This registry and list of objectives creates a research opportunity—do regions that use the registry make more progress on any of these goals than areas that do not use the registry, controlling for selection effects of which areas do and do not use it?

The factors that may help circumvent corruption in developing countries, however, might also help perpetuate it. In particular, the so-called "blockchain governance paradox" suggests that because blockchain can reduce the transaction costs to conducting criminal activity, as discussed above, it can also create new avenues for government corruption.[11]

We can already observe instances of government use of blockchain to enable new avenues of corruption. In particular, it may be an effective method for rogue governments to circumvent international sanctions or conduct illicit activity.[12] In Venezuela, central bankers have issued a cryptocurrency called a "Petro,"[13] that some believe is a means for evading U.S.

[10] https://bitcoinmagazine.com/articles/de-soto-inc-where-eminent-domain-meets-blockchain/
[11] https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/
[12] https://www.cnbc.com/2018/02/22/iran-becomes-latest-rogue-state-to-develop-its-own-cryptocurrency.html
[13] https://www.reuters.com/article/us-venezuela-economy-cryptocurrency/u-s-warns-investors-over-venezuelas-petro-cryptocurrency-idUSKBN1F52AB

sanctions on Venezuela.[14] North Korea reportedly uses cryptocurrencies as a mechanism for earning hard currencies.[15]

A large literature studies the effectiveness of international sanctions. Blockchain technology may have large effects on the effectiveness of such sanctions. On the one hand, they may make sanctions more effective if they make it possible to keep records of transactions. On the other hand, they also give states additional ways of countering sanctions. Researchers might find fertile ground studying the net effects of blockchain on sanctions and state-sponsored corruption.

Outdated Institutions

In principle, blockchain may yield large benefits where technology related to the underlying asset has outpaced existing institutions and the relevant stakeholders agree a new system is necessary. When do benefits of a new technology make a change in existing institutions possible?

Music licensing may be one such example. Obtaining the rights to distribute music in the digital era is exceedingly difficult due to rules that in some cases are over a century old. Sometimes the rights to a given musical piece are split between a large number of rights holders, or worse, often nobody knows who holds the rights to any given music. Rights holders may include major artists and labels but might also include amateur musicians with no representation.

Again, a distributed ledger seems, on paper at least, a way to handle some of these problems. Of course, while blockchain may lower transaction costs to help an artist monetize their songs, the ledger itself will not increase market demand for the music. But aggregations of small music royalties may stimulate creative production. If songs can be monetized, perhaps

[14] http://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/
[15] https://www.vox.com/world/2018/2/28/17055762/north-korea-sanctions-bitcoin-nuclear-weapons

more creators who otherwise would stay on the sidelines will enter the market and produce quality output, through learning-by-doing and improvement over time.

Some groups are building blockchain-based music rights aggregation systems.[16] They may or may not succeed, and that outcome will be determined by the net expected benefits of the innovation and the reaction by the various existing stakeholders. The evolution of a single industry is not necessarily conducive to empirical research, but a detailed examination of the interplay of various groups may provide insight into the challenges facing new institutions even when facing outdated, costly incumbent systems.

III. Humans in the Blockchain

One problem inherent in blockchain is akin to Arrow's Impossibility Theorem, which states that it is impossible to construct coherent societal preferences from individuals' preferences without violating a key component of a democratic system. Someone, for example, must decide the method of voting, which imposes a single person's preferences on the choice method, thereby affecting the outcome. Similarly, blockchains do not appear from thin air. Several aspects of human involvement may undermine the potential benefits of blockchain.

One way humans can undo potential benefits is at the point where they must enter the relevant data into a computer system in the first place. In Sierra Leone, for example, a Swiss blockchain startup company used blockchain to track the results of an election. The company claimed in a press release that blockchain would provide "a secure and transparent digital voting system to enhance [the]…electoral process…. This election highlights blockchain's potential to ensure a permanent, transparent and secure record of votes."[17] In reality, the experiment

[16] https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again
[17] https://agora.vote/pdf/Agora_Press-release_SL2018.pdf

highlighted why blockchain does not necessarily yield benefits in reality despite its theoretical advantages. In this case, citizens handwrote their ballots and handed them to officials, who then manually typed the results into a private blockchain ledger.[18] The method thus retained all previous possible avenues for corruption while adding others, as well as opportunities for manual transcription errors.

Another way humans influence the process is that someone must choose the protocols the blockchain uses. Even architects of cryptocurrencies acknowledge that, "Bitcoin will require the emergence of governance structures, contrary to the commonly held view in the Bitcoin community that the currency is ungovernable" (Kroll et al., 2013, at 1). The human element remains – at some point in the design and development of blockchain, a consensus of rules is needed to determine "which transactions and blocks are considered valid and which are not." (*Id.* at 15).

A key question for researchers, then, is to identify the types of human interactions with blockchain that increase or reduce error or otherwise affect the efficiency of the blockchain.

IV. Conclusions

Blockchain has benefits and costs, and as with any technology, can exacerbate or mitigate weaknesses in existing institutions. The new technology has implications for research in new institutional economics and transaction cost economics, particularly in property rights and corruption studies. A vast array of non-market activities may be measured, exchanged, and monitored with blockchain. New institutional economists may find a new world of resource

[18] https://www.technologyreview.com/the-download/610520/sierra-leones-blockchain-vote-sounds-neat-but-dont-get-carried-away/

economics to study. However, blockchain is best understood at the margin in improvements to economic efficiency and governance.

Blockchain is partly revolutionary and partly hype, raising similar questions about technology and institutions that have been raised before. Because so few "revolutionary" technologies turn out to be so, it is unlikely that blockchain will dismantle and replace the modern state. Yet, we cannot know the effects for certain, and the largest effects are likely to be from applications we cannot predict. But researchers face a plethora of opportunities to help us identify and understand the imagined and real economic effects of blockchain.

References

Arruñada, B. (2018). "Blockchain's Struggle to Deliver Impersonal Exchange," *Minnesota Journal of Law, Science & Technology*, 19(1): 55-150 (2018), *available at* https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1438&context=mjlst.

Catalini, C., and J. Gans. (2016). "Some Simple Economics of the Blockchain," NBER Working Paper No. 22952, http://www.nber.org/papers/w22952.

Catalini, C., and J. Gans. (2018). "Initial Coin Offerings and the Value of Crypto Tokens," MIT Sloan Research Paper No. 5347-18, Rotman School of Management Working Paper No. 3137213, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3137213.

Gans, J., and H. Halaburda. (2013). "Some Economics of Private Digital Currency," in *Economic Analysis of the Digital Economy*, National Bureau of Economic Research, Chicago: University of Chicago Press, http://www.nber.org/chapters/c12992.pdf.

Kroll, J., I. Davey, and E. Felten. (2013). *The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, available at* http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf.

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

Williamson, S. (2018). "Is Bitcoin a Waste of Resources?," Federal Reserve Bank of St. Louis, Early Edition, 2018, https://research.stlouisfed.org/publications/review/2018/02/13/is-bitcoin-a-waste-of-resources/.