https://doi.org/10.1142/9789811220470_0001

Chapter 1

A Brief Introduction to Blockchain Economics

Long Chen*, Lin William Cong[†,§] and Yizhou Xiao[‡]

*Luohan Academy, Xixi Road Hangzhou, China

[†]Cornell University, Ithaca, NY, USA

[‡]Chinese University of Hong Kong, Hong Kong

[§]will.cong@cornell.edu

Abstract

We introduce economic research on blockchains and its recent advances. In particular, we highlight the (i) unifying concepts on blockchain as a decentralized consensus and its core benefits, (ii) equilibrium characterizations and allegedly irreducible tensions among consensus formation, decentralization, and scalability, (iii) major issues including network security, overconcentration, energy consumption and sustainability, adoption, multi-party computation and encryption, smart contracting, and information distribution and aggregation, and (iv) future directions concerning blockchains and their applications such as informational and agency issues, as well as game-theoretical and mechanism design approaches to blockchain protocols.

Keywords: Bitcoin; Consensus protocol; Cryptocurrency; Distributed ledger; Smart contracts.

1. Introduction

The advancement in technology has made us increasingly connected in this digital age. Also undeniable is the corresponding increase in the demand for peer-to-peer interactions that are instantaneous and open, which can transform how people work, consume, and invest. Some of the most valued companies in the world such as Amazon, Alibaba, and Facebook all connect dispersed users and product/service providers. They also give rise to the so-called "gig/sharing economy" wherein on-demand labor gets instantaneous payments instead of relying on long-term employment contracts that are confined by geography and legal jurisdictions.

Integral to this development is digitization of information, which can be broadly interpreted to include digitization of assets too because a digital asset such as a Bitcoin is in principle a string of numbers and alphabets (or 0s and 1s) after all. Because digitized information is non-rival and can be transferred, used, and reproduced almost costlessly, it transcends traditional boundaries of firms and organizations and physical locations, drastically increasing the quantity and quality of economic activities and reshaping business organizations.

While digital technology helps overcome limits in offline markets, digitization alone is insufficient. While smartphones and online apps providing instant access to goods together with virtually unlimited access to wireless high-speed broadband connections all seem to exponentially grow connectivity and lower the cost of segmentation for many industries' production processes (e.g., Fort, 2017), successful platforms and production organizations still depend heavily on payment and contracting innovations (e.g., Taobao and eBay) as the lack of trust among anonymous agents or in an open system is the key obstacle for economic exchanges.

Recently, instead of relying on financial systems that are often arranged around a series of centralized parties like banks and payments, clearing and settlement systems, blockchain-based cryptoapplications attempt to resolve the issue by creating the financial architecture for peer-to-peer transactions and interactions and reorganizing society into a series of decentralized networks. By providing decentralized consensus, blockchains allow peers distant from and potentially unknown to one another to interact, transact, and contract without relying on a single centralized trusted third party. It also holds the potential to better coordinate and organize oft-segmented individuals and groups, thus fully unleashing the

latent productivity hidden in traditional economies due to localized information and geographical constraints.

Technically speaking, blockchain is just one of the many distributed ledger technologies. It first became popular due to the emergence of the cryptocurrency Bitcoin. It has since manifested itself in various other forms, often with the ability to store and execute computer programs. This gave rise to applications such as smart contracts, featuring payments triggered by a tamperproof consensus of contingent outcomes and financing through initial coin offerings. Among many other applications, Maersk and IBM used blockchain for tracking and better logistics in freight shipping and trade credit; Walmart also worked with IBM for supply chain delivery; Stellar and Ripple have revamped the payment and remittance system; Ant Financial implemented blockchain-based cross-border transfers in 2018 and electronic receipts in medical insurance in 2019, among others (Luohan Academy, 2019). Blockchains have also found applications in the areas of healthcare and insurance (Yermack, 2017; Yue *et al*., 2016; Raikwar *et al*., 2018). Media articles and research papers such as those by Chiu and Koeppl (2019), Cong and He (2018), and Reese (2017) contain other examples of blockchain applications. We neither repeat the existing and potential applications of the technology nor elaborate on the technical details that computer scientists have discussed extensively. Instead, we focus on the key economic issues brought forth by the technological innovations and associated applications.

A discussion of blockchain invariably appears incomplete without talking about cryptocurrencies and tokens. Indeed, there is as much novel economics in the use of cryptotokens as there is in the blockchain infrastructure and architect. We leave it out for separate discussions for two reasons. First, we want to correct the misconception that cryptocurrency and blockchain are equivalents or interchangeable. Second, a fast-emerging literature studies cryptocurrencies and cryptotokens, either jointly with blockchain or independent of the technical aspects of decentralized ledgers. In some regard, cryptocurrencies and tokens are also closely related to the literature on monetary economics, banking, and platform economics. It is impossible to reproduce a complete list of relevant articles here and doing so would take too much focus away from our main topic. We therefore refer the readers to studies such as those by Cong *et al*. (2018b), Chod and Lyandres (2018), Liu and Tsyvinski (2018), Cong *et al*. (2019), Gan *et al*. (2019), Lyandres (2019) and the references therein for further discussion. In particular, the study by Halaburda and

Sarvary (2016) gives an excellent overview of digital currencies and that by Cong (2019) provides a concise introduction to the economics of tokens and digital currency.

Our paper is not meant to be a survey of research on blockchains. Instead, our goal is to first clarify from an economic perspective what blockchains are (or envisioned to be) and why they are (or would be) useful and then introduce a generalized concept of desirable features together with a conjecture of their irreducible tension. We then highlight key economic issues surrounding blockchains before pointing out future research directions and challenges to tackle in practice. For more comprehensive surveys, interested readers may consult Townsend (2019) for an insightful overview of DLTs; Hilary and Liu (2018) for a general survey of research on blockchain economics; Tschorsch and Scheuermann (2016) and Conti *et al*. (2018) for discussions on security privacy issues; Biais *et al*. (2019b) and Liu *et al*. (2019) for game-theoretical analyses on blockchains; and Halaburda and Haeringer (2018) for economic and computer science studies specifically related to Bitcoin.

The remainder of the paper is organized as follows: Section 2 defines the general concept of blockchain and explains its main advantages over traditional systems. Section 3 introduces protocol games and design before highlighting the three desirable features of blockchain design and the seemingly irreducible tension among them. Section 4 examines key economic issues surrounding the technology, such as network security, energy consumption, and adoption limitation, with a particular effort to underscore two hitherto underexplored information-related dimensions i.e., information distribution and aggregation in decentralized systems, as well as the innovation of permissioned blockchains in enabling better multi-party computation and information exchanges. Finally, Section 5 summarizes promising future directions for research and for industry development.

2. Blockchain as Decentralized Consensus

To start to comprehend blockchain economics, one has to first understand the general definition of blockchains, their main functionalities and advantages, and the major tradeoffs in achieving all desirable features associated with it. Not surprisingly, the myriad definitions in popular media and emerging economic literature do not help. We aim to provide a

coherent version that facilitates our discussions on the key economic issues related to blockchains.

2.1. *What is blockchain?*

Technically speaking, blockchain is a distributed system that stores time-ordered data in a continuously growing list of blocks. Each block contains information on transactions and business activities, and the entire network uses a consensus algorithm to reach an agreement on which block will be attached to the current recognized chain of blocks, thus the name "blockchain".

The blockchain technology is a manifestation of the more general distributed ledger technology (DLT), which embodies the infrastructure and process for a network to generate a consensus record of state changes or updates to a synchronized ledger distributed across various nodes in the network. Another popular form of DLT is the directed acyclic graph (DAG), often considered to be a rival technology to and an enabler for blockchain. Unlike blockchains that organize records in an unalterable, chronological order, DAGs represent networks of individual records linked to multiple other transactions. In technical jargon, a blockchain is a linked list, whereas a DAG is a tree, branching out from one record to another, and so on.[1] While the discussion to follow often applies equally to other DLTs, we encourage the readers to focus on blockchains for concreteness. In that sense, "blockchain" can be viewed as a general reference for systems of decentralized consensus.

Blockchains can be public (also referred to as open or permissionless), permissioned, or private. The distinction is more about who gets to participate in the consensus formation process, rather than the users of particular applications. Public blockchains typically allow any agent to potentially be a consensus recordkeeper via the protocol and randomization; permissioned blockchains have a prespecified group of recordkeepers; and private blockchains retain their irreversibility and tamper resistance property, but are mostly proprietarily maintained. Most cryptocurrencies (e.g., Bitcoin)

[1] DAG accommodates larger numbers of users and faster transaction times, but does not establish a strict ordering of transactions and would require additional layers of protocols.

are based on public blockchains, whereas many enterprise applications rely on permissioned/consortium blockchains.

Blockchain enthusiasts argue that the technology provides many functions, such as secure data storage and anonymity. Because solutions to these problems are abundant outside of the blockchain space, the impact of blockchain along these dimensions, although material, is somewhat incidental. In our opinion, the core functionality of the technology lies in the provision of decentralized consensus. Consensus here refers to agreements not only on transactions but also on protocols for conflict resolution, history of events, institutional memory, etc.

The concept of consensus is not alien to economic and social functions. It is the informational basis for agents of divergent preferences and beliefs to agree on the states of the world or behave according to a common set of protocols. Its benefits for and empowerment of everyone sharing and trusting the same ledger are apparent: Settlements in some cases no longer take days, lemons problems and frauds can be mitigated, and the list goes on. Traditionally, centralized parties such as courts, governments, and notary agencies provide such consensus, but in a way that could be labor intensive, time consuming, and prone to tampering and monopoly power. Blockchains provide an alternative, decentralized way of generating consensus information. It is important to recognize that decentralization here entails both the way consensus is generated and the way it is distributed and stored. For example, Bitcoin mining under proof-of-work generates consensus, and information about the newly appended block is also stored on multiple (if not all) nodes representing network participants' computers.

All blockchains, to a large extent, aim to create an infrastructure for decentralized or multi-centered agents or institutions to interact and jointly record and maintain information, with no individual party exercising persistent market power or control. One defining feature of blockchain architectures is therefore their ability to allow decentralized recordkeepers to maintain a uniform view on the state of things and the order of events — a decentralized consensus (Cong and He, 2018). We should reckon that decentralization is a matter of degree. Public blockchains tend to be completely decentralized by freely admitting users and recordkeepers. In contrast, permissioned or consortium blockchains have a restricted set of recordkeepers and may have restrictions on who may use the blockchain or access information therein. Nevertheless, it could be more decentralized than traditional systems such as individual banks.

In a broader sense, blockchains aim to provide a trusted system or environment for economic agents to interact. "Trusted" in computer science means carrying out transactions in a fault-tolerant way. The consideration of blockchain economics and its link with trust brings a whole new perspective. For example, a decentralized trustworthy system may allow better search and matching in storage sharing or world computing without high intermediary costs (Filecoin and Dfinity are among current attempts); it may also coordinate various interested parties without concerns on who runs the show or whether a particular political/legal framework has ulterior motives (Libra and Ethereum which do not belong to any particular country or company are some cases in point despite the fact that Facebook or Vitalik Buterin are taking a lead in the development).

2.2. *Benefits of decentralization*

If centralized systems such as governments and large IT firms have traditionally supplied trusted systems and digital platforms/exchanges, why do we need decentralized consensus in the first place? To this question, many articles provide a misleading or incomplete picture, overemphasizing transparency or anonymity. While Bitcoin is well-known for its anonymity and thus associations with illegal activities such as money laundering and drug dealing, anonymity is a design feature rather than a defining characteristic of blockchains in general. We attempt to give a definitive answer and highlight the three core benefits of decentralization. Note that in many cases and applications, decentralization manifests itself in the form of multi-centers.

2.2.1. *Preventing single point of failure*

It is widely accepted that a decentralized system prevents or reduces what is called "single point of failure" (SPOF). SPOF is a part of a system that, upon failing, prevents the entire system from functioning. SPOFs are undesirable in any system requiring continuity and reliability, be it a business practice or software application. By having irreversible records distributed to decentralized notes, blockchains in a sense help mitigate SPOFs because no single node's failure is likely to disable the entire network and consensus process.

While this benefit seems to contradict the observed hacking of crypto exchanges and the DAO attack of a former decentralized autonomous organization, we remind the readers that these incidents happened to centralized wallets and accounts. If the system were truly decentralized and peer-to-peer, such massive failures would be less likely to occur even when a few nodes are hacked. In that regard, it is not whether a decentralized system mitigates the problem of SPOF, but about whether a system is decentralized, a topic we visit in Sections 3 and 4.

Because hash-pointers give immutability (with time stamping) and tamper resistance, no single party can go back in history to change the records or the sequence of events. This is useful for maintaining a consistent global consensus history, which can be used for contingency references for smart contracting. There are costs though, as we point out in Sections 3 and 4. For one, storing duplicate copies of entire history of transactions could be costly. Decentralized consensus protocol may also entail excessive energy consumption.

More importantly, we argue that the concept of SPOFs should be more broadly interpreted. Beyond technical SPOF, such as the breakdown of a computer, or wiping out of corporate facilities due to natural disasters, SPOF here can refer to economic incentives. For example, it is easier to bribe a single judge for a court case than bribing an entire panel of judges. Hack and theft of credit card data target a specific database or an individual. Facebook's leakage of data to Cambridge Analytica and Google's fine of 57 million euros for failing to comply with GDPR (https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/) are also examples of SPOF in business in which the action or negligence of a centralized platform leads to system wide debacles. Had the consensus process on how to handle data belonged to a decentralized set of agents, such violations may have been prevented by a majority of agents who are more sensitive to data privacy issues.

2.2.2. *Reducing market power and enabling stakeholding*

Another popular argument for adopting the blockchain technology centers around disintermediation. This is at best a misnomer. In fact, decentralized systems could allow intermediaries to thrive because they also allow more efficient search and match for intermediaries with end customers. What people have in the back of their minds is that blockchain systems are

typically open, which allows easier entry and more competition to improve efficiency and reduce intermediary rent. Moreover, it could enable P2P transactions that would be infeasible under traditional systems and therefore filling in missing markets. This is a point Townsend (2019) belabors, for good reasons.

Another warranted clarification is that even though decentralized systems such as blockchains reduce market power, it is a matter of degree. It certainly does not imply that the market would be perfectly competitive. In fact, Cong *et al*. (2018) show that even mining pools enjoy some local monopoly. Similarly, while the openness nature of many blockchain systems would blur the boundary of legal jurisdictions or physical geography, it is most likely that regional regulations are still relevant (a case in point is the ban on cryptocurrency exchanges by China and South Korea). The relevant question is to what extent do they matter. More importantly, what is novel relative to traditional centralized systems is that the consensus mechanism (specifically node leader elections) leaves little room for any single party to have persistent market power or governance authority over time.

The reduction in market power concentration also reflects in a novel fashion on the consensus mechanism that existing studies and media articles rarely touch on. In many business-to-customer (B2C) businesses, consumers or platform users generate invaluable information and network externality that the business platforms tap without explicitly compensating the end users. For example, Facebook and Google monetize users' social interactions and emails, yet it is often difficult for users, especially early adopters, to share the economic surplus of such business behemoths. Greater competition would lead businesses to seek alternative ways to attract users and early adopters.

Traditionally, a platform would provide tools to empower network participants. For example, Alibaba's Tmall Innovation Center (TMIC) began in 2016 to help brands design products for consumers by utilizing its online surveys. Tao Factory helps coordinate smart supply chain for its 40,000 factories from more than 30 industries, so that they have the ability to quickly adjust its assembly lines to unanticipated changes in customer demand.

One novel way is to have users be stakeholders of the future prosperity of the businesses or platforms. Blockchains enable a trusted way of distributing digitized securities or cryptotokens to early adopters and users, even when the distributing businesses are still little known.

This enables businesses to return value to consumers for the contributions they make on platforms or open-source projects.

2.2.3. *Enabling value exchange, asset traceability, and information interaction*

It is crucial to recognize that we live in a digital age with abundant data. In that sense, a trust system for interaction concerns not only the exchanges of value or objects but also the exchanges of information. Blockchain provides the building blocks for a trust system based on digital information and algorithms.

Because permissioned blockchains and private blockchains do not have open access, many economists question whether a lot of the excitement about blockchain is merely excitement about database upgrade.[2] We would like to point out that even permissioned and private blockchains represent important innovations rather than mere database upgrades for the following reasons: the consensus generation process, though not fully decentralized, is often more decentralized than traditional systems; more importantly, the immutability of blockchain records coupled with proper encryption algorithms can enable proprietary databases (permissioned nodes or private blockchains) to interact to produce useful information aggregation, verification, and exchanges, all without sacrificing data privacy.[3] This was difficult to achieve before the introduction of secure multi-party computation, one of the most important developments in computer science over the past few years. It also allows us to enhance traceability of offline assets/products by recording their origination and path of ownership in a tamperproof manner (e.g., Alibaba's IoT Global Origin Traceability Plan; Luohan Academy, 2019).

Through smart contracts (e.g., using Solidity, a popular programming language used on Ethereum), programs that run on blockchains, one ensures that only transaction parties can execute the transaction using digital signature based on asymmetric keys, without the intervention of

[2] See, for example, https://review.chicagobooth.edu/economics/2018/article/blockchain-s-weakest-links and Halaburda (2018).

[3] Data privacy is particularly important in, for example, healthcare and financial services (Yue *et al*., 2016; Raikwar *et al*., 2018).

any trusted third party. This further allows agents in a blockchain network to exchange digital assets or share the surplus generated through information aggregation or exchange. In a similar vein, blockchains, whether open or not, can potentially allow exchanges of offline objects when combined with internet of things (IoTs) (Popov, 2016; Ali *et al*., 2018; Bakos and Halaburda, 2019).

To be concrete, Section 4.5 provides an example of blockchain architecture for collaborative auditing (Cao *et al*., 2018). Encryption algorithms such as the zero-knowledge-proof (ZKP) on top of blockchains allow auditing firms to exchange encrypted information so that they can audit transactions while preserving client firms' proprietary information. R3 has developed ready-to-use permissioned blockchain infrastructure that can integrate with clients' Enterprise Resource Planning (ERP) systems with a reasonable adoption cost. Promising start-ups such as the Oasis Lab and Duality are other examples of blockchain applications in multi-party computations (MPCs).

It is worth mentioning that all three advantages of the blockchain system together enable it to be an ideal infrastructure for non-profit and social projects.[4] Blockchains' three benefits also create "liquidity" for many hitherto illiquid assets or items. For example, the reliable and timely recording of receipts and account receivable in a decentralized network imply that agents in the system can use these assets for collateral or transfer of value in ways that a traditional system fails to achieve (just think about how long it takes for a travel reimbursement to be deposited into your account before you can use the resource). This would affect banks' rehypothecation business as well.

3. Consensus Generation and Economic Tradeoffs

Consensus protocols are essentially the rules of the game for agents in distributed computing and multi-agent systems, so that they can agree on records that are needed to achieve overall system reliability in the

[4]See, for example, https://www.thenonprofittimes.com/technology/blockchain-gaining-ground/. Ant Financial has also been leading the effort to apply the technology to the philanthropy sector (https://www.newsbtc.com/2016/07/31/alibaba-groups-ant-financial-creates-blockchain-solution-for-philanthropy-sector/).

presence of agent heterogeneity (faulty nodes or processes are just special examples). For blockchains, the best-known consensus protocol is proof-of-work (PoW), which is behind Bitcoin's design.

True to the Stigler's Law of Eponymy, the ingredients and principles for Bitcoin were introduced much earlier, and Nakamoto's innovation truly lies in putting it altogether (Narayanan and Clark, 2017). Early attempts at cryptocurrencies lacked a proper incentive system for decentralized nodes to properly record transactions, either because they needed some oversight (e.g., entity to have final decision on penalties) or because they did not constrain coin issues (uncontrolled inflation) (Halaburda and Sarvary, 2016). This leads to double-spending issues that would invalidate the digital currency in question. Nakamoto introduced the concept of bitcoin mining (essentially the PoW), in which independent computers (miners) dispersed all over the world spend resources and compete repeatedly for the right to record new blocks of transactions, and the winner in each round gets rewarded. Independent miners have incentives to honestly record transactions because rewards are valid only if their records are endorsed by subsequent miners. The avoidance of double spending in turn validates bitcoins as a form of payment in the network.

In this section, we start with a discussion on PoW before introducing alternate protocols and important tradeoffs among various desirable features of blockchain.

3.1. *Games under consensus protocols*

Consensus protocols have been studied for decades in the field of computer science. While in computer science and modern cryptography we typically make assumptions on the actions of the agents (an honest node behaves honestly; a faulty node always misbehaves), economists tend to make assumptions on the primitives such as agents' utility functions and then analyze their strategic behaviors in equilibrium. What economics brings to the table for consensus protocols are the concepts of equilibrium (and potential multiplicity), incentive compatibility (Bitcoin's mining protocol is an instance of incentive compatible protocol), and mechanism design. These in turn allow us to talk about incentives in a large or open system, in order to achieve general resilience and feasibility of the decentralized systems.

3.1.1. *Proof-of-work protocol*

Agents in the economy are not machines, and therefore providing them the right incentives for proper recordkeeping is crucial. PoW at present is the predominant protocol for generating decentralized consensus. Recordkeepers here are the miners around the world who compete for the right to record a brief history (known as a block) of bitcoin transactions. The winner gets rewarded with a fixed number of bitcoins (currently 12.5 bitcoins), plus any transaction fees included in the transactions within the block (Easley *et al*., 2017). Miners utilize computation power to solve cryptographic puzzles in order to win the competition, which resembles effortful mining activities.

Two features are common in PoW protocols. First, the difficulty of the cryptopuzzles dynamically adjusts so that the speed of block generation and thus recording is limited. In the case of Bitcoin, one block is generated on average every 10 min. This means that recordkeeping is an arms race: devoting more computation power improves the chance of winning the recordkeeping right but does not increase social surplus. Moreover, there is necessarily usage congestion because the system throughput is limited. Although not optimally designed, difficulty adjustments are not *ad hoc* and do serve the purpose of network security and are essential for raising revenue from users to fund miners provision of infrastructure (Huberman *et al*., 2017).

Second, in addition to getting newly minted native tokens, miners in many PoW blockchains also receive fees attached by users. In the case of Bitcoin, there is the transition from mining new bitcoins to getting market-based fees (Easley *et al*., 2017). Given the rising importance of transaction fees and that fee structure could also lead to instability of the system (e.g., Carlsten *et al*., 2016), how to determine them in a market mechanism as part of the protocol design constitutes an interesting problem. Basu *et al*. (2019) were pioneers of such a discourse.

Nakamoto envisioned that when appending blocks, the winning miner would append to the longest chain, thus the "longest chain rule". Here is the heuristic argument: Because miners receive block rewards and fees in native tokens and the receipt is only valid if others continue building from the block they build, miners have incentives to properly record because otherwise others will not follow the block record. Forking out on her own is also not attractive because she is in a tournament with the entire mining community and it is highly likely that a fraudulent branch would be

shorter than the one that the rest of the community accepts. There are also other heuristics practiced in the blockchain community such as the "first-seen rule" which says that all miners add blocks to the heaviest chain of which they know, using the first branch it has heard of as tiebreaker. What is implicit in these folk theorems is a vague notion of equilibrium.

Kroll *et al*. (2013) were among the earliest to study whether following the longest chain rule is a Nash equilibrium. Biais *et al*. (2019a) further fully formalized the strategic actions of players involved and demonstrated that even without majority computation power, a miner can attack the system to make it unstable. Having forks also delays consensus because persistent forking eventually leads to the splitting of the blockchain, as seen in the case of Ethereum and Ethereum Classic or Bitcoin and Bitcoin cash.

Consistent with the finding of equilibrium multiplicity by Biais *et al*. (2019a), Eyal and Sirer (2014) discuss how successful miners hide their success and start mining the second block without competition while honest miners are still busy mining the first block. If they succeed mining the second block, they will collect two block rewards, and their chain is the longest block. Even if the honest blockchain finds the first block before the selfish miner finds the second, the selfish miner could release its block immediately to compete for the reward.

Nayak *et al*. (2016) and Kiayias *et al*. (2016) consider generalization and optimal forms of selfish mining strategies in Eyal and Sirer (2014) to include stubborn mining such as forking (building private branch).

One main takeaway from these studies is that equilibria under PoW are far from being well understood. Because of the network security implications and the intellectual curiosity of understanding protocol games, one would expect further studies from both computer scientists and economists along this line of work.

3.1.2. *Alternative protocols*

The largest blockchains (e.g., Bitcoin, Ethereum) employ PoW, but PoW possesses significant shortcomings such as energy cost or bandwidth limit. Various alternatives have been proposed. In fact, PoW is not even among the first consensus protocols. For one, computer scientists have long worked on consensus protocols in a closed or permissioned environment where the number of members is not too big and the members are known. Byzantine fault tolerance (BFT) protocol (Castro and Liskov, 2002)

is well studied and understood when applied to such an environment.[5] Roughly speaking, PoW offers good node scalability but poor performance in terms of processing capacity, whereas variants of BFT offer good performance for small numbers of replicas. They often lack scalability in open environments that blockchains applications typically entail. Practitioners are actively exploring protocols such as practical BFT (pBFT), hybrid BFT, delegated BFT, obfuscated BFT, simplified BFT, and VBFT that combine proof-of-stake (PoS, which we introduce shortly), verifiable random function, and BFT. The recent Facebook Libra stable coin also utilizes a version of BFT as part of the consensus protocol. Game-theoretical models on BFT-based protocols also constitute an important area of research (Amoussou-Guenou *et al*., 2019).

Another popular alternative to PoW is PoS. In PoS-based blockchains, the creator of the next block is chosen via various combinations of random selection and wealth (in native tokens) or age (i.e., the stake). The study by Saleh (2019a) provides the first formal economic model of PoS and establishes conditions under which PoS generates consensus. A sufficiently modest reward schedule not only implies existence of an equilibrium in which consensus is obtained as soon as possible but also precludes a persistent forking equilibrium. The latter result arises because PoS, unlike PoW, requires that validators hold stake. Importantly, Saleh (2019a) dispels the myth of "nothing-at-stake" (malicious nodes lose nothing when behaving badly) through endogenizing native token prices.

Another protocol, proof-of-burn (PoB), has seen recent applications. To win the right to record new blocks, one has to "burn" tokens by sending them to invalid public addresses so that no one can ever use them again. While practitioners probably did not have the following in mind, PoB happens to speak to PoW's exceptional price volatility. Exceptional price volatility arises because PoW implements a passive monetary policy that fails to modulate cryptocurrency demand shocks. Saleh (2019b) theoretically formalized the aforementioned point. PoB implements an active albeit *ad hoc* monetary policy that modulates cryptocurrency demand shocks. PoB is an example of supply-side management of cryptocurrencies, which potentially reduce the welfare loss in PoWs compensating those updating the blockchain through an arms race while facilitating free entry among them. A related study is that by Cong, Li, and Wang (2019),

[5]Readers are encouraged to read more about the Byzantine General's problem.

which fully endogenizes dynamic token supplies and offers a corporate finance perspective of protocol design.

3.2. *Blockchain impossibility triangle?*

It should be apparent to readers that one goal of the blockchain technology is to achieve more decentralization. But for the blockchains to receive wide adoption and application, they also have to ensure that the consensus provision is accurate and scalable. Public blockchains such as the Bitcoin blockchain achieve decentralization and consensus record at the same time, but doing so reduces their scalability. Traditional payment processing tools such as Visa and Mastercard achieve consensus record and scalability, but lack decentralization. Records made in large scales with decentralization are hard to synchronize and achieve consensus. It seems that global consensus, decentralization, and scalability are hard to achieve at the same time.

Vitalik was among the first to put forth the scalability trilemma that is widely recognized among practitioners (Ometoruwa, 2018). The trilemma describes how it is difficult to achieve decentralization, security, and scalability at the same time. Security refers to the level of defensibility a blockchain has against attacks from external sources of linear-order computation power. In fact, Brewer (2000) conjectured even earlier in a talk that it is impossible for a distributed data system to simultaneously provide consistency, availability, and partition tolerance. This was proven later by Gilbert and Lynch (2002).

Abadi and Brunnermeier (2018) gave an insightful and more comprehensive discussion of a similar trilemma from an economic perspective. When a blockchain is decentralized and correct, the lack of dynamic rent by various recordkeepers necessarily implies that the system is costly; when the system is decentralized and maintained at low cost, recordkeepers may misreport; when the consensus is correct and maintenance of the system is cheap, the outcome is incompatible with free entry and information portability (compared with traditional reputation-based system) conditions.

The concept of "security" is just one aspect of consensus, in the sense that the whole system agrees on the state of the world and that agreement cannot be attacked. The tradeoffs do not necessarily involve dynamic considerations as in Abadi and Brunnermeier (2018) either. Moreover, there are more than three dimensions of tradeoffs in the blockchain technology,

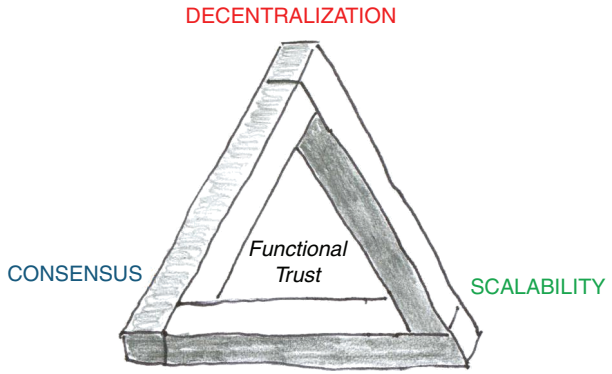

Figure 1: Impossibility triangle.

such as transparency, immediacy, level of adoption, which constitute a rich avenue for future research. Nevertheless, we argue that almost all tradeoffs can be interpreted as manifestations of the tension among decentralization, scalability, and consensus (formation). We conjecture that there is such a general impossibility triangle (Figure 1) and discuss below how this can be a useful framework to think about various tradeoffs in blockchain innovations. As we walk you through the irreducible difficulties that arise when one tries to achieve all three, we also mention how practitioners are still actively working on layer 1 protocol innovations and layer 2 business model innovations to resolve the seeming impossibility triangle.

3.2.1. *Decentralization*

Decentralization in our context means a significant degree of distribution of a system's information, governance, ownership, etc. When decentralized agents jointly make decisions, intuitively it takes a clever design to reach agreements. The more decentralized the system is, the greater the potential failure for reaching a global consensus. Moreover, decentralized storage of global consensus necessarily leads to duplication, be it storage, queries, recordings, etc. In either case, consensus accuracy or system processing capacity would be compromised.

Layer 1 protocol innovations on consensus protocols often come at the expense of decentralization. For example, the variants of conventional

BFTs allow a high number of messages in that every node multi-casts its messages to every other node. Functional separation of leader election and transaction validation allow localization (Eyal *et al*., 2016). Bitcoin runs verification and leader election at the same time, but Bitcoin NG is forward-looking and uses key blocks to elect a leader first who validates transactions in microblocks in the next 10 minutes. Other solutions include forming a committee to vouch for new blocks through BFT (e.g., ByzCoin (Kogias *et al*., 2016)) and sharding (e.g., Elastico (Luu *et al*., 2016)). Sharding makes sense, but requires something called Atomic Cross-Shard Commitment Protocol. All these involve some local consensus formation within a preselected committee instead of open consensus all the time.

3.2.2. *Consensus* (*formation*)

Note that the consensus we have in mind is global consensus that can be used in various applications. This is hard to achieve. In fact, Fischer *et al*. (1982) show that there is no guarantee that an asynchronous network can agree on a single outcome.

One way is to sacrifice efficiency and scalability to wait for a decentralized system to reach consensus. Many permissionless blockchains do this, which we discuss shortly in the next subsection. Another way to overcome the consensus problem is to synchronize from a single point, but this means centralization. We believe that sacrificing some decentralization is a promising direction and enterprise blockchains are going to be the major trend for blockchain applications. Trust combined with efficiency can disrupt existing business models and relationships.

It is worth mentioning that DAG, an alternative architecture to ensure decentralization and scalability, instead sacrifices consensus. In fact, there may not be a global consensus at any given point in time. A hybrid of DAG and blockchain is being explored to enforce collective consensus generation, minimizing the monopolitic power of the round leaders (Abram *et al*., 2019).

3.2.3. *Scalability*

Bitcoin only processes less than five transactions per second, whereas VISA and Mastercard process thousands, not to mention Alibaba's Tmall processes 100 billion RMB worth of transactions under 2 hours on

China's single's day.[6] For blockchains such as the P2P payment Bitcoin network to be widely adopted, they have to effectively scale. Two obvious solutions are increasing the block size or decreasing the block intervals. Increasing the size decreases fairness in that large miners have an advantage (law of large numbers would not play out). It also requires more storage space and network bandwidth, not to mention that it requires more verification time (which is not an issue for simple transactions in bitcoin, but could be an issue when verifications are more complicated). In addition, increasing the block size still does not solve the problem of miners strategically partially filling the blocks (Malik *et al*., 2019). What about decreasing block interval? It would imply that it requires lower computation to attack unless participants increase the confirmation lags correspondingly, leading to more forks and stale blocks all of which result in network instability and inaccurate or unreliable consensus.

Most current applications of blockchains have decentralization and consensus and are battling the scalability issue. Multi-chain solutions increase throughputs at the expense of security; for merge mining, agents share mining power as in the case of Namecoin, where store and computation loads on each node increase, which is similar to block size increase. Other solutions include cross-chain layer 2 innovation, of which Ripple's interledger is a leading candidate, off-chain; state channel, with the best-known example being the Lightning Network, Casper; Sharding "parallel processing", e.g., Ethereum Casper, Zilliqa (open-source); Segwit, DAG.

It should be recognized that depending on the application, we do not need to achieve all three objectives at the same time. Besides exploring solutions to the challenge of the impossibility triangle, another fruitful path could be to clearly identify the need in particular applications and design the protocols and business models correspondingly.

4. Key Economic Issues

Mechanism design and protocol innovations to achieve decentralization, consensus, and scalability have received increasing attention from computer scientists and economists. In this section, we highlight that the

[6]Based on 2018 data and supported by AliPay and OceanBase database. See, for example, http://m.mnw.cn/news/cj/2084010.html and https://tech.sina.cn/2018-11-11/detail-ihmutuea8987030.d.html.

specific designs of consensus protocols can have general social economic implications. These have to be taken into consideration in designing the protocols too.

We start with the well-known discussion in computer science on network security and end with an emphasis on the role of information — an important topic that is inappropriately relegated to the backseat, if not neglected entirely, in many studies.

4.1. *Network security*

The earliest discussions on blockchains took place in the computer science field and largely concern network security. This is very much related to our earlier discussions on protocol games. Once we fix the consensus protocol, there could be a number of strategies that attackers/malicious nodes in the network could deploy. Consider PoW for example. Below, some of the well-known attacks are described.

In denial-of-service (DoS) attack and its derivatives such as distributed DOS, a malicious cyber threat prevents legitimate users from accessing information systems, devices, or other network resources, so as to lower other players' (typically mining pools') profits (Johnson *et al*., 2014).

Besides direct attacks, there could be other forms of instability driven by decentralized miners' incentives. For example, without newly minted bitcoins, miners may extend the blocks with the most available transaction fees rather than to follow the longest chain, causing instability of the network (Carlsten *et al*., 2016).

A much studied case is selfish mining, in which malicious miners or pools withhold the mined blocks. Honest miners then waste their computational power in finding blocks already mined, and malicious miners increase their probability of finding the next block. This leads to majority attack. It is often mentioned that with 51% of the global hash power, one can be a dictator on recordkeeping. What is often the case is that as long as an attacker amasses a large percentage of the global hash power, the system's security is at risk (Sapirshtein *et al*., 2016; Bahack, 2013).

Network security in the blockchain setting can be viewed as robust consensus, and there often features a tension between a more decentralized structure and scalability. Overall, network security issues remain an active area of research for blockchains. Taking a game-theoretical approach has been tremendously helpful for understanding the behaviors

of agents and robustness of the system for a given consensus protocol. We anticipate more mechanism design approach in future that has network security as part of the objective to optimize over candidate designs.

4.2. *Overconcentration*

In addition to network security, the blockchain community has been extremely concerned with overconcentration. For a system with a sufficiently large processing capacity, the incentives for consensus generation seem to lead to an industrial organization with a perceived tendency for concentration. This is aggravated by the emergence of mining pools that combine an individual miner's hash power to solve cryptographic puzzles in PoW and then distribute the rewards. An open blockchain's optimal functioning relies on adequate and sustainable decentralization that cannot be taken for granted. In fact, over time some pools gain a significant share of global hash rates (a measure of computation power), with the mining pool GHash.io briefly reaching more than 51% of global hash rates in July 2014. Therefore, the rise of mining pools in many, presumably distributed cryptocurrency-mining activities calls into question the stability and viability of such systems. Overconcentration therefore runs counter to blockchain advocates' ideology of decentralization.

The study by Cong *et al*. (2018) shows that risk sharing constitutes a natural force against decentralization and gives rise to mining pools. Ferreira *et al*. (2019) show that application-specific integrated circuits (ASICs) that are used for mining could lead to concentration in ASIC production market which then affects the mining pool concentration.

Figure 2 illustrates the evolution of the distribution of hash rates among Bitcoin mining pools. Clearly, overtime mining pools gradually dominate solo mining: mining pools represented less than 5% of the global hash rates at the start of June 2011 but have represented almost 100% since late 2015. This phenomenon suggests that natural economic forces tend towards centralization within a supposedly decentralized system. But an equally interesting fact is that, while large pools do arise from time to time, none of them grow to completely dominate global mining. This observation hints at concurrent economic forces that suppress overcentralization.

Indeed, Cong *et al*. (2018) demonstrate that diversification across pools and the industrial organization of mining pools naturally moderate

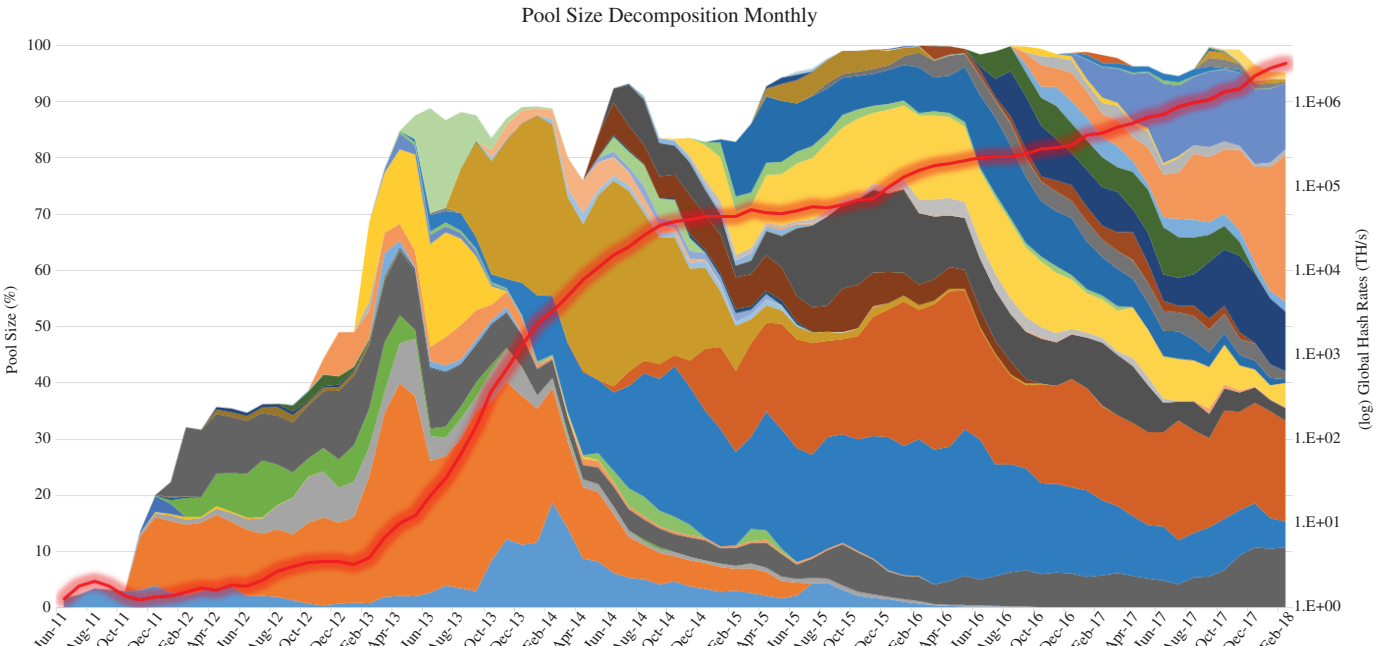

Figure 2: The evolution of size percentages of Bitcoin mining pools.

Notes: This graph plots (1) the growth of aggregate hash rates (right-hand side vertical axis, in log scale) starting from June 2011 to today; and (2) the size evolutions of all Bitcoin mining pools (left-hand side vertical axis) over this period, with the pool size measured as each pool's hash rates as a fraction of global hash rates. Different shades indicate different pools, and white spaces indicate solo mining. Over time, Bitcoin mining has been increasingly taken over by mining pools, but no pool seems to ever dominate the mining industry for long. The pool hash rates data come from Bitcoinity and BTC.com, with details given in Cong *et al*. (2018).

overconcentration of mining power. Intuitively, larger pools have more market power because the risk-sharing benefit it provides is larger. Therefore, pool owners charge higher fees, leading to a smaller percentage growth in pool size. Empirical evidence supports the theoretical predictions. Every quarter, the authors sort pools into deciles based on the start-of-quarter pool size and calculate the average pool share, average fee, and average log growth rate for each decile. They show that pools with larger start-of-quarter size charge higher fees and grow slower in percentage terms. They investigate these relationships in three 2-year spans (i.e., 2012–2013, 2014–2015, and 2016–2017, as shown in Figure 3) and find that almost all of them are statistically significant with the signs predicted by their theory.

The insights from this chapter can be extended to other protocols such as PoS, because miners in PoS systems also form coalitions (e.g., Brunjes *et al*., 2018).

4.3. *Energy consumption and sustainability*

The issue surrounding blockchains that has received the most attention is arguably the energy implications for PoW-based blockchains. The purported advantages of Bitcoin are dwarfed by the intentionally resource-intensive design in its transaction verification process which threatens the environment integral to our survival.[7] Environmental science and engineering studies have estimated the detrimental environmental impacts of cryptomining (e.g., Li *et al*., 2019; de Vries, 2019; Truby, 2018). Again, this is a manifestation of the impossibility triangle: for a large-scale decentralized system, generating consensus could be very costly.

A number of economic studies also recognize that the mining game in PoW-based blockchains is essentially an arms race due to difficulty adjustments in many of the consensus protocols. Basically agents acquire more computation power to compete in a fixed-sum game because more global hash power does not lead to more native coins or tokens being minted and distributed to the miners. O'Dwyer and Malone (2014); Chiu

[7]Energy issues are also related to scalability, but they are not exactly the same. For one, even if Bitcoin processes way more transactions or way less transactions, energy consumption could be high if coinbase is worth a lot and many miners started competing.

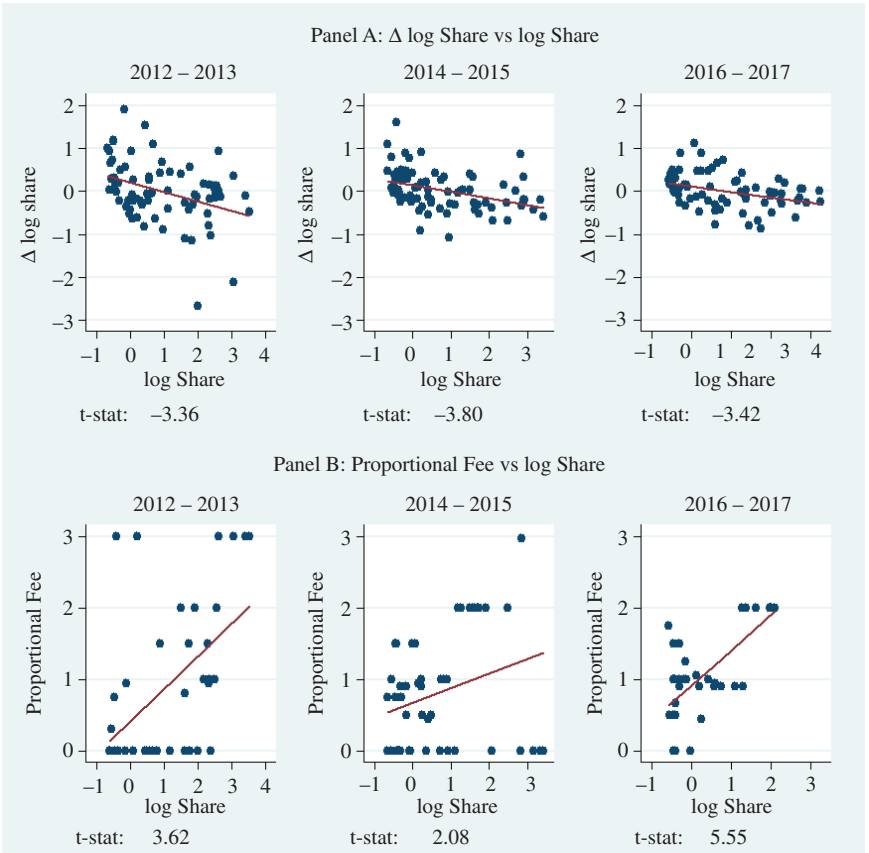

Figure 3: Empirical relationships of pool sizes, fees, and growths.

Source: Reproduced from Cong *et al*. (2019).

Notes: This figure shows the binned plots of the changes in logShare (Panel A) and Proportional Fees (Panel B) against logShare. Share is the quarterly beginning (the first week) hash rate over the total market hash rate. Fees are the quarterly averaged proportional fees. Within each quarter t; $\text{logShare}_{i;t+1}$, Proportional $\text{Fee}_{i;t}$, and $\text{logShare}_{i;t}$ are averaged within each $\text{logShare}_{i;t}$ decile, and these mean values are plotted for 2012–2013, 2014–2015, and 2016–2017. Solid lines are the fitted OLS lines, with t-stat reported at the bottom. Data sources and descriptions are given in their paper.

and Koeppl (2017); Ma and Tourky (2018); Cong *et al*. (2018); Pagnotta (2018); Prat and Walter (2018); Saleh (2019a) all acknowledged that greater global mining does increase the network security, but the energy used may have greater social benefit when deployed elsewhere.

In particular, Benetton *et al*. (2019) found empirical evidence that cryptomining crowds out other economic activities and may result in net welfare loss. Using data from various cities in China and New York State, the authors found large negative externalities of cryptomining on the local economy, such as distortion to local wages and electricity price. As the study by Benetton *et al*. (2019) points out, local taxes would only drive the problem elsewhere, akin to the phenomenon of corporate profit shifting to tax-friendly geographies, while worldwide levy is hard to coordinate.

Given that the current designs for Bitcoin and the like entail a large social welfare loss, but can be improved with more efficient design, practitioners have attempted to channel the computation to scientific problems. For example, in proof of useful work or resources (PoUWR), the mining computation is used for performing stochastic gradient descent for neural network training (Bottou 1991). Not all scientific computation problems are NP-complete, which is required for many PoW protocols, the energy problem remains.

Most studies hint at cryptocurrency price and mining cost as the biggest drivers on the global mining activities. Intuitively, the higher the Bitcoin price, the more entry and greater computation power miners use, which leads to a higher energy consumption. This is only an incomplete description in that in the long run, compensation is driven by system congestion and market fees attached by the users. If Bitcoin is worth more, users just attach less number of bitcoins. In that regard, Bitcoin price cannot be the long-term and only driver for the high energy consumption.

This is where mining pool is included in the discussion. For the same amount of monetary rewards, if miners' risk-bearing capacity is greater, then they devote more mining power — another key insight in Cong *et al*. (2018). Figure 4 demonstrates that when mining pools help miners to share risk, the aggregate mining could easily double for realistic parameters for Bitcoin mining. For further discussion on the dynamic evolution of distribution of miners and reward schemes in mining pools, we refer the readers to Liu *et al*. (2018) and Fisch *et al*. (2017). It is yet to be seen how consensus protocol innovations resolve the issues created by mining pools.

4.4. *Adoption*

In some sense, blockchain's scalability is reflected by endogenous user adoptions. Without user adoption, most blockchain applications cannot

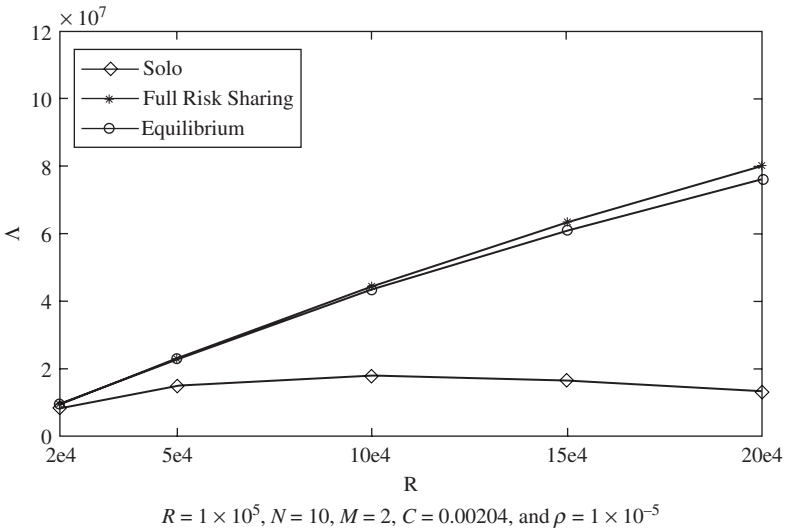

Figure 4: Global hash rates under solo mining, full-risk sharing, and mining pool equilibrium.

Source: Reproduced from Cong *et al*. (2019).

Notes: Here R is the mining reward, C is related to mining cost, and ρ is risk aversion. M and N are parameters for the number of mining pools and the number of solo miners.

survive over the long run. Athey *et al*. (2016) carried out one of the earliest studies that take users' adoption into consideration, with an emphasis on the role of learning in agents' decisions to use Bitcoins. While Athey *et al*. (2016) did not consider users' network externality, Cong *et al*. (2018b) took network externality and blockchain platform's productivity into consideration to analyze token pricing and the roles of tokens. They derived a fundamental token pricing formula and showed that adoption of blockchain platforms crucially depends on the underlying technology and transaction needs.

Hinzen *et al*. (2019) also demonstrated that a limited adoption problem arises endogenously in PoW blockchains. Increased transaction demand increases the fees, which induce recordkeepers to enter the network (for permissionless blockchains). The increased network size then protracts the consensus process and delays transaction confirmation. Users adopt only if they possess extreme insensitivity to delays, limiting a PoW payments blockchains widespread adoption. The authors then argue that permissioned blockchain can overcome this problem because there is

no difficulty adjustments or free entry of recordkeepers. However, validators may still collude, which can be solved by a stake-based voting rule.

4.5. *Multi-party computation and permissioned blockchains*

Multi-party computation (MPC) has been extensively studied for decades because it enables computation with correctness while preserving privacy. Its implementation has been challenging because the strong assumptions on agents' honesty means in practice it is prone to SPOFs (such as DoS attacks), not to mention that scaling in a large (often open) system is costly (Zyskind *et al*., 2016). As described earlier, one of Nakamoto's innovations lies in introducing incentives into a consensus system. This way, the blockchain technology offers a form of incentive compatibility that mitigates both problems.

Specifically, blockchains can potentially serve as a trusted settlement layer to discipline malicious behaviors (through verifying transcripts of computations). They also allow introducing some randomization of committee selections (sometimes referred to as quorums) at a low cost, which can potentially scale MPC networks efficiently. Alex Pentland, the founder of MIT Media Lab and one of the most prominent data scientists, was quoted as saying, "[With blockchains, now] you can get insights across countries, across data holders, without exposing individual data and without disobeying either privacy or data localization laws" (MIT, 2018).

Permissioned blockchains are widely used as a distributed database system that could enable MPC. Many industries, such as auditing and financial report, can potentially benefit from the technology. Auditing has its unique need for a customized system to protect clients' information privacy. Such a need leads many auditors to develop permissioned blockchains independently as a database upgrade (Tysiac, 2018). Yet, with up-to-date and immutable historical record, auditors can easily verify the transactions on blockchain ledgers (either because the transactions are public or because they are on an auditor's proprietary blockchain or other private blockchains that auditors have access to) instead of asking clients for bank statements or sending confirmation requests to third parties. Moreover, communications across auditors could greatly improve auditing efficiency if the auditors automate information verification of clients' transaction with minimum sharing of their clients' information with other auditors, thanks to zero-knowledge protocols that preserve data privacy and integrity.

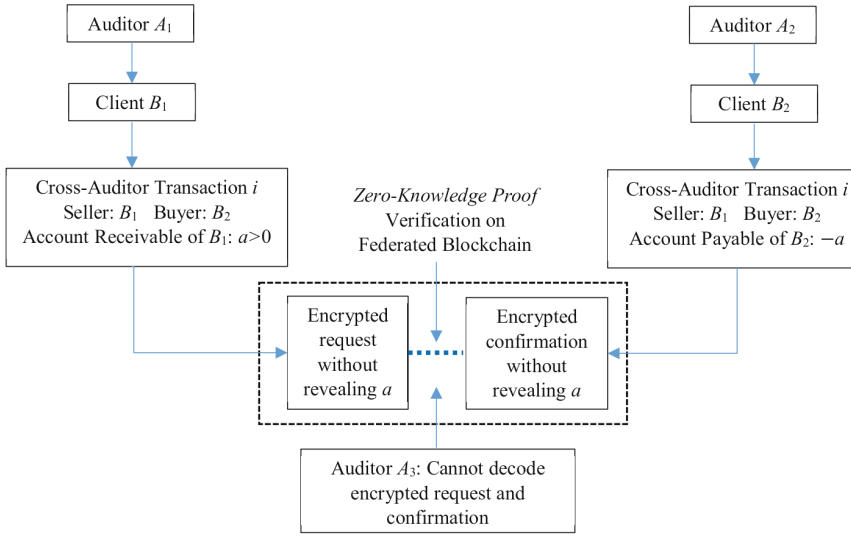

Figure 5: Transaction verification on a P2P federated blockchain.

Source: Reproduced from Cao *et al*. (2019).

Cao *et al*. (2018) provide a blueprint for such collaborative auditing using a federated blockchain which reduces auditing costs not only for transactions recorded on their proprietary databases but also for cross-auditor transactions. Figure 5 provides an illustration. Specifically, information providers in this federate blockchain system technically do not share any client transaction information except for providing a confirmation to information requesters. Other auditors cannot infer any information about the clients or the transactions from the request or the confirmation. This collaboration among auditors does not require a third party to monitor or intermediate. Once auditors request information through this federated blockchain framework, it is difficult for any auditor or outside hackers to intentionally revise or delete the information because the information is distributed to all auditors. Such immutable nature of information also makes it easier for the regulator to inspect auditors' auditing process.

The authors then model auditor competition for clients, allowing endogenous audit quality and clients' misstatement, before discussing regulatory policy in a unified framework to understand the implications of blockchain for auditing. They find blockchains lead to more real-time verification of transaction records on blockchains, forcing firms to misreport more in

off-blockchain records. The reduction in auditing cost allows auditors to respond by inspecting a higher fraction of off-chain records and discretionary accounts. Overall, auditors spend less on auditing and reduce misstatement risk. Auditors charge competitive fees to attract clients, which are lower when using federated blockchains. But fees depend on both the transaction volume and counterparties' auditor association. Auditors' adoption of the technology also exhibits strategic complementarity in the sense that one auditor's adoption encourages others to adopt. To rule out the inefficient outcome where no auditor adopts the technology, a regulator can encourage or require adoption to enhance welfare and reduce regulatory costs.

In general, building multi-party computation using the blockchain infrastructure remains a promising avenue for blockchain innovations. Data Market Austria (https://datamarket.at/en/ueber-dma/) is a recent large-scale endeavor in that direction. That said, while permissioned blockchains allow scalability, they do so at the expense of partial decentralization.

4.6. *Smart contracting*

Smart contracts have received much media hype. While a universally accepted definition for smart contracts has yet to be reached, their core functionality is clear: transfer at little cost or even automate value transfers based on a decentralized consensus record of the states of the world. Cong and He (2018) define them as digital contracts allowing terms contingent on decentralized consensus that are tamperproof and typically self-enforcing through automated execution. Other similar definitions can be found in Szabo (1998) and Lauslahti *et al*. (2017).

To the extent that contract terms are contingent on outcomes that can be recorded on blockchains (potentially via IoTs, or "oracles" feeders of information from the offline world onto the internet), smart contracts foremost reduce the contracting frictions and costs of a trust system. It allows contracting parties to more easily reach consensus which is robust to agency issues or technical failures of recordkeepers. This enlarges the contracting space and makes contracts in practice more complete. Moreover, the linked-list structure and time stamping also allow smart contracts to commit to no renegotiation. In that regard, smart contracts can be robust to renegotiation. Cong and He (2018) and Tinn (2018) formally discussed these issues. Gans (2019) and Bakos and Halaburda (2019) further described how smart contracts can help overcome holdup issues and contracting difficulties, or be integrated with IoT.

Smart contracts' impact on dynamic moral hazard is unclear and is closely related to information design. In particular, more transparency or more frequent monitoring/disclosure of information is not necessarily desirable (e.g., Orlov, 2018). The study by Tinn (2018) contains an in-depth discussion on how learning can make debt and equity more costly and restrictive under moral hazard and relates smart contracting to traditional dynamic moral hazard (e.g., Holmstrom and Milgrom, 1987).

As for broader applications, smart contracts can be designed for information-constrained insurance or credit, in addition to being a device that facilitates information and mechanism design to overcome the issues of rational herding (Cong and Xiao, 2019). Various informational issues such as how blockchain helps with coordination are just starting to be explored; contracting using digital information is likely an important ingredient in the overarching architecture. They, in turn, are related to competition and industrial organization. Lyandres (2019) is a recent examination of the effects of price commitments via smart contracts on firm competition and value.

As much as we are excited about the potential of smart contracting, we have to recognize their limitations. First, it cannot enforce the transfer of ownership of offline assets, a point also belabored in Abadi and Brunnermeier (2018); second, it has been combined with IoTs and oracles to acquire information off-chain; third, it is not a panacea for incomplete contracting: contingencies traditional contracts cannot specify are also hard to program into smart contracts, unless artificial intelligence drastically changes how smart contracts function.

Once again, consensus for smart contracting at large scale may make decentralization difficult due to the implications of information distribution, a point that we will discuss next.

4.7. *Information aggregation and distribution*

Closely related to smart contracting is the broader informational implication of blockchains, an aspect of the technological development that is largely neglected. Economists have long understood that information distribution or disclosure could lead to undesirable outcomes such as collusions (Bloomfield and O'Hara, 1999). Cong and He (2018) were also among the first set of researchers to bring such discussions to blockchains

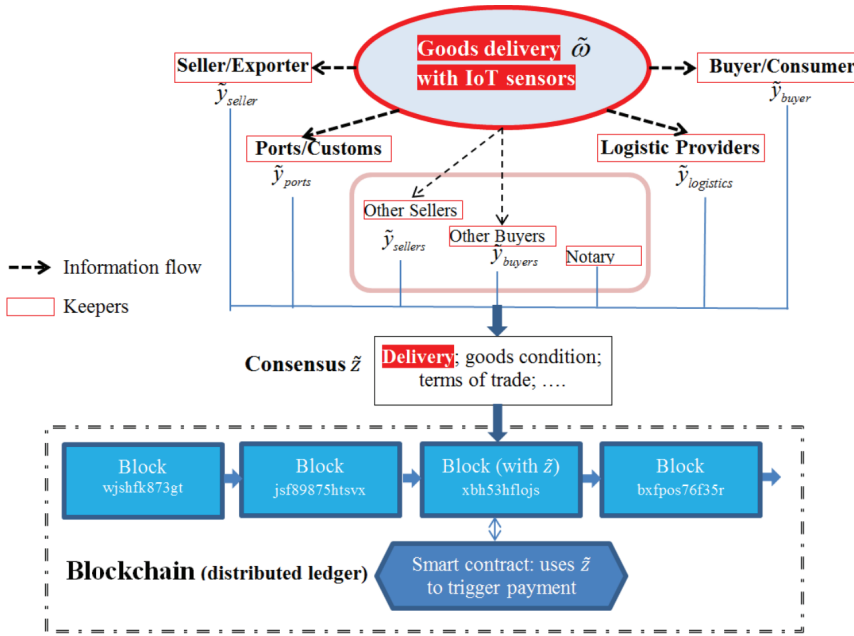

Figure 6: A diagram of the trade finance example of a blockchain.

Source: Reproduced from Cong and He (2019).

Notes: A seller delivers goods to a buyer, with $\tilde{\omega}$ denoting the contingency of successful delivery. Recordkeepers, potentially with real-time IoT sensors, monitor the delivery and submit their reports, $\tilde{y}_k$'s. The protocol of blockchain aggregates these reports to form a decentralized consensus, $\tilde{z}$. This consensus, together with the smart contract, is stored in the block and then added to the blockchain.

and point out considerable informational challenges in maintaining a decentralized system.[8]

The main insight in Cong and He (2018) is that in order for a decentralized consensus system to be robust to single points of failure, there has to be some degree of information distribution, even encrypted information. This is illustrated in Figure 6. But greater information in the public domain would lead to market participants to tacitly collude more, hurting consumer welfare.

[8]A related study is by Aune *et al*. (2017), who discussed the use of hashing to secure time priority without revealing detailed information and disclosing information later, in order to prevent front-running a transaction.

Though the information distribution entailed in decentralized consensus processes could be detrimental, the authors' message is broader: the robust decentralized consensus enables agents to contract on delivery outcomes and automate contingent transfers, therefore eliminating information asymmetry as a barrier for entry and encouraging greater competition. Blockchains and smart contracts expand the set of possible dynamic equilibria leading to social welfare and consumer surplus that could be higher or lower than in a traditional world.

Information transmission is also affected by the technology. For example, Chod *et al*. (2019) show that signaling a firm's fundamental quality (e.g., its operational capabilities) to lenders through inventory transactions is more efficient than signaling through loan requests. The blockchain technology could enable the verification of fundamentals and provide greater transparency into a firm's supply chain.

Finally, blockchain architecture can also be utilized for crowdsourcing and information aggregation. Indeed, many blockchain-based platforms increasingly use token-weighted voting to crowdsource information from their users for content curation, on-chain governance, etc. The role of decentralized structure and tokens are yet to be fully understood. For example, Falk and Tsoukalas (2019) have showed that token weighting generally discourages truthful voting and erodes the platform's information aggregation for prediction.

5. Concluding Remarks and Future Directions

To conclude, we summarize the key takeaways of the discussion thus far. Digital technology rebuilds the dynamics and relations among economic agents, potentially turning competition to collaboration, integrating segmented markets, and enabling consumers to participate and benefit more from business enterprises. Digitized information and functional trust constitute the hallmarks of a digital economy. While great progress has been achieved in terms of digitization, building trust on digital networks has been challenging. Blockchains provide a potential decentralized solution. Against this general backdrop, several general themes on blockchain economics stand out.

First, a game-theoretical approach to understanding consensus protocols has proven successful. For example, Biais *et al*. (2019b) point out directions in setting fees and designing throughput capacity, etc. The key is to specify preferences and action space, and agents rationally maximize their expected utilities. This is different from computer scientists' typical

approach of directly assuming nodes' behaviors. One case is the study by Manshaei *et al*. (2018), who studied multiple committee runs in parallel to validate a non-intersecting set of transactions (a shard), with both Byzantine agents and rational agents. Amoussou-Guenou *et al*. (2019) have analyzed a similar problem in a dynamic setting and showed that rational agents can be pivotal instead of merely free ride.

Among the attempts at resolving the various bottlenecks of blockchain systems, those that involve local consensus, local centralization, or local scalability for solving privacy issues, saving storage, increasing throughput seem promising (Sharding is an example). Elastico (NUS Singapore) is an example. Each committee that uses BFT then submits the summaries to the final committee.

Second, besides technical innovations aimed at overcoming the impossibility triangle, breakthroughs are likely to come from mechanism design approaches to consensus protocols, with clear objectives for specific applications. For example, some blockchain applications may not require scalability, while some do not require global consensus. The protocol designs would differ correspondingly. Wishful ideology or Utopian dreams of full decentralization are not going to effectively propel the industry forward, but the right designs incentivizing and empowering agents in a decentralized or multi-centered system will.

In particular, protocol design should take into consideration blockchain governance (not only consensus about transactions but also how to resolve conflicts such as forking). One recent attempt related to governance and voting schemes was that of Barrera and Hurder (2018). A mechanism design approach also allows us to link layer one (decentralized consensus) and layer two (business model) innovations. Some designs could be useful for both incentivizing consensus generation and incentivizing users, as we elaborate next.

Third, agency and incentive issues remain at the core of blockchain economics. The discussion of incentive provision should not be restricted to the consensus protocol level, but can be extended to include user adoption, market design, etc., that are at the platform/ecosystem level.

Here, smart contracts coupled with sensors/IoTs would prove useful in that they can ensure prompt and guaranteed payments when contingent terms are satisfied. Would more verifiable data improve contracting efficiency? A better traceability of product and cash flows may allow firms to collateralize their account receivables more effectively and to receive payments from banks more quickly. They can also be used to compensate

contributors and users on the network for content contributions and the like or between organizations such as mining pools and their members.

Speaking of users, their decision-making in a decentralized system is less studied, so are entrepreneurial teams that build the blockchain infrastructures. The interaction of user and consensus provision, and more generally, the service provision and demand in a platform economy can bring new economic insights for blockchain applications. The use of cryptotokens may prove useful in aligning incentives on platforms.[9] The work by Cong *et al*. (2018a) serves as an example of a recent study in this direction.

Finally, informational exchanges and data issues here started to be explored. In initial coin offerings (ICOs) or initial exchange offerings (IEOs), how would the informational asymmetry and environment relate to misreporting, incentive alignments, and fraudulent activities? How should policymakers regulate the markets and mandate information disclosures? How do we utilize IoTs and oracles to input information from offline environments? How would protocol designs matter for information aggregation and distribution?

In particular, the decentralized system seems to offer a solution for achieving data privacy and effective use of proprietary databases at the same time. Multi-party computation combining blockchain and various encryption methods opens new doors for how data are stored and used across institutions and individuals in future, which in turn affects economic decision-making. One caveat is that blockchains alone are not panacea for the problem of offline data authenticity and original data quality.

Surveying the past and looking into the future, we can say that if information and assets are the blood of a human body, then trust/consensus system (centralized or decentralized) is the vessel. Similarly if big data and physical resources are the input for the society's production, a functional digital network is the production function. Distributed systems such as blockchains are likely to be an integral part of this broader picture.

[9]While media discussions focus on cryptocurrencies as a substitute for money, it is equally important to understand the fundamental economics of using tokens on platforms or at digital market places. A large number of industry projects and academic studies are devoted to understanding better tokenomics, which could be just as important as blockchain protocol designs.

Acknowledgments

The authors thank Hanna Halaburda and Maureen O'Hara for detailed feedback and suggestions. They are also grateful to Bruno Biais, Jonathan Chiu, Evgeny Lyandres, and Fahad Saleh for helpful comments. This research was funded in part by the Ewing Marion Kau man Foundation. The contents of this publication are solely the responsibility of the authors.

References

Abadi, J. and M. Brunnermeier (2018), Blockchain economics, Discussion paper, mimeo Princeton University.

Abram, M., D. Galindo, D. Honerkamp, J. Ward, and J.-M. Wong (2019), Democratising blockchain: A minimal agency consensus model, working paper.

Ali, M. S., M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani (2018), Applications of blockchains in the internet of things: A comprehensive survey, *IEEE Communications Surveys & Tutorials* **21**(2), 1676–1717.

Amoussou-Guenou, Y., B. Biais, M. Potop-Butucaru, and S. Tucci-Piergiovanni (2019), Rationals vs byzantines in consensus-based blockchains, arXiv preprint arXiv:1902.07895.

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

Aune, R. T., A. Krellenstein, M. O'Hara, and O. Slama (2017), Footprints on the blockchain: Trading and information leakage in distributed ledgers, *The Journal of Trading* **12**(3), 5–13.

Bahack, L. (2013), Theoretical bitcoin attacks with less than half of the computational power (draft), arXiv preprint arXiv:1312.7013.

Bakos, Y. and H. Halaburda (2019), When do smart contracts and IOT improve efficiency? Automated execution vs. increased information, Automated Execution vs. Increased Information (May 26, 2019), NYU Stern School of Business.

Barrera, C. and S. Hurder (2018), Blockchain upgrade as a coordination game.

Basu, S., D. Easley, M. O'Hara, and E. Sirer (2019), Towards a functional fee market for cryptocurrencies, Available at SSRN 3318327.

Benetton, M., G. Compiani, and A. Morse (2019), Cryptomining: Local evidence from China and the US, Working paper.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019a), The blockchain folk theorem, *The Review of Financial Studies* **32**, 1662–1715.

Biais, B. (2019b), Strategic interactions in blockchain protocols: A survey of game-theoretic approaches, Working Paper.

Bloomfield, R. and M. O'Hara (1999), Market transparency: who wins and who loses?, *Review of Financial Studies* **12**, 5–35.

Bottou, L. (1991), Stochastic gradient learning in neural networks, *Proceedings of Neuro-Nimes* **91**, 12.

Brewer, E. A. (2000), Towards robust distributed systems, Principles of Distributed Computing, Portland, Oregon Invited Talk.

Brunjes, L., A. Kiayias, E. Koutsoupias, and A.-P. Stouka (2018), Reward sharing schemes for stake pools, arXiv preprint arXiv:1807.11218.

Cao, S., L. W. Cong, and B. Yang (2018), Auditing and blockchains: Pricing, misstatements, and regulation, Misstatements, and Regulation.

Carlsten, M., H. Kalodner, S. M. Weinberg, and A. Narayanan (2016), On the instability of bitcoin without the block reward, in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp. 154–167.

Castro, M. and B. Liskov (2002), Practical byzantine fault tolerance and proactive recovery, *ACM Transactions on Computer Systems* (*TOCS*) **20**, 398–461.

Chiu, J. and T. V. Koeppl (2017), The economics of cryptocurrencies — bitcoin and beyond, Working Paper.

Chiu, J. (2019), Blockchain-based settlement for asset trading, *The Review of Financial Studies* **32**, 1716–1753.

Chod, J. and E. Lyandres (2018), A theory of ICOs: Diversification, agency, and asymmetric information, Working paper Boston University Questrom School of Business.

Chod, J., N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber (2019), On the financing benefits of supply chain transparency and blockchain adoption, Management Science.

Cong, L. W. (2019), A brief introduction to tokenomics, Palgrave Handbook of FinTech and Blockchain Book Chapter under Preparation.

Cong, L. W. and Z. He (2018), Blockchain disruption and smart contracts, Forthcoming, Review of Financial Studies.

Cong, L. W. and J. Li (2018), Decentralized mining in centralized pools, Working Paper.

Cong, L. W., Y. Li, and N. Wang (2018a), Token-based corporate finance, Working Paper.

Cong, L. W. (2018b), Tokenomics: Dynamic adoption and valuation, Working Paper.

Cong, L. W. (2019), Tokenomics and platform finance, Working Paper.

Cong, L. W. and Y. Xiao (2019), Information cascades and threshold implementation, University of Chicago, Becker Friedman Institute for Economics Working Paper.

Conti, M., E. Sandeep Kumar, C. Lal, and S. Ruj (2018), A survey on security and privacy issues of bitcoin, *IEEE Communications Surveys & Tutorials* **20**, 3416–3452.

de Vries, A. (2019), Renewable energy will not solve bitcoins sustainability problem, *Joule* **3**, 893–898.

Easley, D., M. O'Hara, and S. Basu (2017), From mining to markets: The evolution of bitcoin transaction fees, Working Paper.

Eyal, I., A. E. Gencer, E. G. Sirer, and R. Van Renesse (2016), Bitcoin-ng: A scalable blockchain protocol, in *13th fUSENIXg Symposium on Networked Systems Design and Implementation* (*fNSDIg 16*), pp. 45–59.

Eyal, I. and E. G. Sirer (2014), Majority is not enough: Bitcoin mining is vulnerable, in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 436–454.

Falk, B. and G. Tsoukalas (2019), Token weighted crowdsourcing, Discussion paper, Working Paper.

Ferreira, D., J. Li, and R. Nikolowa (2019), Corporate capture of blockchain governance, Available at SSRN 3320437.

Fisch, B., R. Pass, and A. Shelat (2017), Socially optimal mining pools, in *International Conference on Web and Internet Economics*, Springer, pp. 205–218.

Fischer, M. J., N. A. Lynch, and M. S. Paterson (1982), Impossibility of distributed consensus with one faulty process. Discussion paper, Massachusetts Inst of Tech Cambridge lab for Computer Science.

Fort, T. C. (2017), Technology and production fragmentation: Domestic versus foreign sourcing, *The Review of Economic Studies* **84**, 650–687.

Gan, J. R., G. Tsoukalas, and S. Netessine (2019), Inventory, speculators and initial coin offerings, The Wharton School Research Paper.

Gans, J. S. (2019), The fine print in smart contracts, Discussion paper, National Bureau of Economic Research.

Gilbert, S. and N. Lynch (2002), Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services, *Acm Sigact News* **33**, 51–59.

Halaburda, H. (2018), Blockchain revolution without the blockchain, Bank of Canada Staff Analytical Note 5.

Halaburda, H. and G. Haeringer (2018), Bitcoin and blockchain: What we know and what questions are still open, NYU Stern School of Business, Forthcoming.

Halaburda, H. and M. Sarvary (2016), Beyond bitcoin, *The Economics of Digital Currencies*, Springer.

Hilary, G. and L. Liu (2018), Blockchain and nance, Working paper.

Hinzen, F. J., K. John, and F. Saleh (2019), Bitcoin's fatal aw: The limited adoption problem, NYU Stern School of Business.

Holmstrom, B. and P. Milgrom (1987), Aggregation and linearity in the provision of intertemporal incentives, *Econometrica: Journal of the Econometric Society* **55**(2), 303–328.

Huberman, G., J. Leshno, and C. C. Moallemi (2017), Monopoly without a monopolist: An economic analysis of the bitcoin payment system, Working Paper 17–92, Columbia Business School.

Johnson, B., A. Laszka, J. Grossklags, M. Vasek, and T. Moore (2014), Game-theoretic analysis of DDoS attacks against bitcoin mining pools, in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 72–86.

Kiayias, A., E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis (2016), Blockchain mining games, in *Proceedings of the 2016 ACM Conference on Economics and Computation*, ACM, pp. 365–382.

Kogias, E. K., P. Jovanovic, N. Gailly, I. Kho, L. Gasser, and B. Ford (2016), Enhancing bitcoin security and performance with strong consistency via collective signing, in *25th fUSENIXg Security Symposium* (*fUSENIXg Security 16*), pp. 279–296.

Kroll, J. A., I. C. Davey, and E. W. Felten (2013), The economics of bitcoin mining, or bitcoin in the presence of adversaries, in *Proceedings of WEIS*, vol. 2013, Citeseer.

Lauslahti, K., J. Mattila, and T. Seppala (2017), Smart contracts — how will blockchain technology affect contractual practices?, Etla Reports.

Li, J., N. Li, J. Peng, H. Cui, and Z. Wu (2019), Energy consumption of cryptocurrency mining: A study of electricity consumption in mining cryptocurrencies, *Energy* **168**, 160–168.

Liu, X., W. Wang, D. Niyato, N. Zhao, and P. Wang (2018), Evolutionary game for mining pool selection in blockchain networks, *IEEE Wireless Communications Letters* **7**, 760–763.

Liu, Y. and A. Tsyvinski (2018), Risks and returns of cryptocurrency, Working Paper 24877, National Bureau of Economic Research.

Liu, Z., N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim (2019), A survey on blockchain: A game theoretical perspective, *IEEE Access* **7**, 47615–47643.

Luohan Academy, Research Team (2019), Digital technology and inclusive growth, Report.

Luu, L., V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena (2016), A secure sharding protocol for open blockchains, in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 17–30.

Lyandres, E. (2019), Product market competition with crypto tokens and smart contracts, Available at SSRN 3395441.

Ma, J., J. S. Gans, and R. Tourky (2018), Market structure in bitcoin mining, National Bureau of Economic Research Working Paper.

Malik, N., M. Aseri, P. Vir Singh, and K. Srinivasan (2019), Why bitcoin will fail to scale?, Available at SSRN 3323529.

Manshaei, M. H., M. Jadliwala, A. Maiti, and M. Fooladgar (2018), A game-theoretic analysis of shard-based permissionless blockchains, *IEEE Access* **6**, 78100–78112.

MIT, M. (2018), Machine learning for encrypted blockchains — Sandy Pentland, Ph.D. thesis.

Narayanan, A. and J. Clark (2017), Bitcoin's academic pedigree, *Communications of the ACM* **60**, 36–45.

Nayak, K., S. Kumar, A. Miller, and E. Shi (2016), Stubborn mining: Generalizing selfish mining and combining with an eclipse attack, in *2016 IEEE European Symposium on Security and Privacy* (*EuroS&P*), IEEE, pp. 305–320.

O'Dwyer, K. J. and D. Malone (2014), Bitcoin mining and its energy footprint, in *IET Conference Proceedings*.

Ometoruwa, T. (2018), Solving the blockchain trilemma: Decentralization, security & scalability, www.coinbureau.com/analysis/solving-blockchain-trilemma/.

Orlov, D. (2018), Frequent monitoring in dynamic contracts, Discussion paper, working paper.

Pagnotta, E. (2018), Bitcoin as decentralized money: Prices, mining rewards, and network security, Mining Rewards, and Network Security (October 26, 2018).

Popov, S. (2016), The tangle, cit. on p. 131. https://files.bitscreener.com/downloads/wp/iota_Whitepaper.pdf.

Prat, J. and B. Walter (2018), An equilibrium model of the market for bitcoin mining, Working Paper.

Raikwar, M., S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay, and K.-Y. Lam (2018), A blockchain framework for insurance processes, in *2018 9th IFIP International Conference on New Technologies, Mobility and Security* (*NTMS*), IEEE, pp. 1–4.

Reese, F. (2017), Land registry: A big blockchain use case explored. Coindesk, April **19** (2017).

Saleh, F. (2019a), Blockchain without waste: Proof-of-stake, Discussion paper, working Paper.

Saleh, F. (2019b), Volatility and welfare in a crypto economy, Available at SSRN 3235467.

Sapirshtein, A., Y. Sompolinsky, and A. Zohar (2016), Optimal sel sh mining strategies in bitcoin, in *International Conference on Financial Cryptography and Data Security*, Springer, pp. 515–532.

Szabo, N. (1998), Secure property titles with owner authority, Online at http:// szabo. best. vwh. net/securetitle. html.

Tinn, K. (2018), "Smart" contracts and external financing, Available at SSRN 3072854.

Townsend, R. (2019), Distributed ledgers: Innovation and regulation in financial infrastructure and payment systems, Discussion paper, Working Paper.

Truby, J. (2018), Decarbonizing bitcoin: Law and policy choices for reducing the energy consumption of blockchain technologies and digital currencies, *Energy Research & Social Science* **44**, 399–410.

Tschorsch, F. and B. Scheuermann (2016), Bitcoin and beyond: A technical survey on decentralized digital currencies, *IEEE Communications Surveys & Tutorials* **18**, 2084–2123.

Tysiac, K. (2018), How blockchain might affect audit and assurance, *Journal of Accountancy* **15**.

Yermack, D. (2017), Corporate governance and blockchains, *Review of Finance* **21**(1), 7–31.

Yue, X., H. Wang, D. Jin, M. Li, and W. Jiang (2016), Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, *Journal of Medical Systems* **40**, 218.

Zyskind, G. *et al*. (2016), Efficient secure computation enabled by blockchain technology, Ph.D. thesis Massachusetts Institute of Technology.