Review of Finance, 2017, 1–24
doi: 10.1093/rof/rfw074

OXFORD

Corporate Governance and Blockchains*

David Yermack

NYU Stern School of Business and National Bureau of Economic Research

Abstract

Blockchains represent a novel application of cryptography and information technology to age-old problems of financial record-keeping, and they may lead to far-reaching changes in corporate governance. Many major players in the financial industry have began to invest in this new technology, and stock exchanges have proposed using blockchains as a new method for trading corporate equities and tracking their ownership. This essay evaluates the potential implications of these changes for managers, institutional investors, small shareholders, auditors, and other parties involved in corporate governance. The lower cost, greater liquidity, more accurate record-keeping, and transparency of ownership offered by blockchains may significantly upend the balance of power among these cohorts.

JEL classification: G23, G32, G34

Keywords: Blockchains, Corporate governance, Shareholder activism, Executive compensation

1. Introduction

This paper explores the potential corporate governance implications of blockchain technology. A blockchain is a sequential database of information that is secured by methods of cryptographic proof, and it offers an alternative to classical financial ledgers. After an explosion of interest from industry in late 2015, blockchains have captured the attention of the business world, as they offer a new way of creating, exchanging, and tracking the ownership of financial assets on a peer-to-peer basis. Major stock exchanges are exploring the

* For helpful comments, I thank seminar and conference participants at the University of Adelaide, University of Amsterdam, Bank of England, University of Bristol, Cambridge University Center for Alternative Finance, Cardiff University, Concordia University, Erasmus University Rotterdam, University of Exeter, Imperial College London, International Organization of Securities Commissions Committee on Emerging Risk, Jesus College Cambridge, London Business School, Melbourne University, University of New South Wales FIRN Corporate Finance Conference, New York University, Queensland University, the University of South Australia, Texas A&M University, the University of Western Australia, and the US Securities and Exchange Commission, as well as Alex Edmans (the editor). Campbell Harvey and Clifford Holderness (the referees), Scott Stornetta, Tim Swanson, and Paul Zarowin. Part of this paper was written while I was a visiting professor at Erasmus University Rotterdam.

use of blockchains to register and trade shares of stock issued by corporations. Blockchains also have the potential to accommodate debt securities and financial derivatives, which can be executed autonomously as "smart contracts," possibilities which are the basis of ongoing pilot projects involving some of the world's largest financial institutions. Further applications may exist in government record-keeping of databases for land titles, vital statistics, and many other areas.

These innovations may affect owners and managers of public companies in important ways, potentially changing corporate governance as much as any event since the 1933 and 1934 Securities Acts in the USA. In this paper, I identify in more detail how the use of blockchains could affect corporate governance from the perspective of corporate managers, institutional investors, debt investors, auditors, and other groups. I also discuss issues related to the internal governance of blockchains themselves, a topic that could become important to corporations in the way that the organization of stock exchanges and other capital market institutions is important today.

Blockchains were proposed by Nakamoto (2008) as a method of validating ownership of the virtual currency bitcoin.[1] After 7 years of successful use with bitcoin, blockchains have become recognized as an alternative to ownership ledgers based on classical double-entry bookkeeping. Blockchains offer potential advantages in cost, speed, and data integrity compared with classical methods of proving ownership, and the scale of these potential savings has motivated investments by venture capitalists and by established players in the financial services industry. Entrepreneurs are actively investigating blockchains' suitability for recording ownership of a wide range of assets, from stocks and bonds to real estate, automobile titles, luxury handbags, and works of art. Further applications under study by governments include using blockchains for public records such as real estate titles, birth certificates, driver's licenses, and university degrees.

Using blockchains to record stock ownership could solve many longstanding problems related to companies' inability to keep accurate and timely records of who owns their shares (Kahan and Rock, 2008). Future extensions could allow blockchains to hold self-executing smart contracts, such as stock options held by employees or warrants owned by outside investors. These smart contracts could extend into areas such as the pre-contracted resolution of financial distress. Perhaps most importantly, blockchains could provide unprecedented transparency to allow investors to identify the ownership positions of debt and equity investors (including the firms' managers) and reduce the opportunity for rent-seeking or corrupt behavior by regulators, exchanges, and listed companies.[2] If a firm elected to keep some or all of its financial records on a public blockchain, as proposed by some commentators,

1 The idea of a blockchain was introduced in Haber and Stornetta's (1991) proposal for the digital time stamping of documents in sequence to authenticate authorship of intellectual property, as discussed below. The first reference to this data structure a "chain of blocks" appears to come from Nakamoto (2008), whose innovations with bitcoin included the connection of the blockchain concept to a public ledger jointly updated by numerous participants in an open-source network.

2 Countless examples of corrupt behavior attributed to banks, exchanges, and regulators have tended to undermine public confidence in financial markets for as long as they have existed. In recent years, these have included the NASDAQ odd-eighths scandal (1994), the technology stock IPO scandal (2002), the after-hours mutual fund trading scandal (2003), the LIBOR manipulation scandal (2011), the foreign exchange front-running scandal (2013), and the gold and silver fixing scandals (2014), among others.

opportunities for accrual earnings management and other financial reporting strategies could drop dramatically, and related party transactions would become much more transparent.

For shareholders, blockchains could offer lower costs of trading and more transparent ownership records, while permitting visible real-time observation of transfers of shares from one owner to another. For activists, the technology could allow for quicker, cheaper acquisitions of shares, but with possibly far less secrecy than under the current system. Activists could also liquidate their positions more easily and more transparently, which might make the "exit" channel of corporate governance increasingly attractive at the expense of the "voice" or intervention channel. Managerial ownership could become much more transparent, with insider buying and selling detected by the market in real time, and manipulations such as the backdating of stock compensation becoming much more difficult, if not impossible, since participants in certain blockchains are unable to "rewrite history" by changing their entries retroactively. Corporate voting could become more accurate, and strategies such as "empty voting" that are designed to separate voting rights from other aspects of share ownership could become more difficult to execute secretly. Any and all of these changes could dramatically affect the balance of power between directors, managers, and shareholders. However, their impact will depend importantly on the type of blockchain used, whether public and freely open to anyone, as is the case with bitcoin and other digital currencies, or restricted and "permissioned," the model currently being tested by a number of established financial institutions and consortiums.

To date the most high-profile proposed use of blockchain technology in corporate finance has occurred in the Australia, where the Sydney-based Australian Securities Exchange in January 2016 announced its intention to redesign its clearing and settlement systems using blockchain technology. Earlier stage investigations of how blockchains could be used in stock markets were announced previously by the US NASDAQ and the Frankfurt Deutsche Borse exchanges.[3] Lee (2016) discusses the potential benefits of blockchains to a stock exchange in such areas as cost and speed of execution and settlement. Schroeder (2015) analyzes the legal basis for treating virtual assets on blockchains as "uncertificated securities" under Article 8 of the Uniform Commercial Code. In the area of shareholder voting, one of the topics discussed later in the paper, the Estonian stock exchange (a unit of the US-based NASDAQ) began in 2016 to conduct shareholder voting on a blockchain platform. In late 2016, a US Public Company, Overstock.com, began taking subscriptions for an equity rights issue over a private blockchain.

Emerging markets may be among the first to see blockchain technology integrated into their stock exchanges and capital markets on a large-scale basis. The prediction of early adoption in developing countries rests upon the convergence of three forces: inadequacy of existing record-keeping systems, mistrust of corrupt and ineffective market regulators, and high penetration of information technology such as smartphones. As examples, the rapid growth of mobile payment systems such as M-Pesa and BitPesa in Kenya,[4] and the recent explorations by the governments of Honduras and the Republic of Georgia of moving their

3 See Hope, Bradley and Casey, Michael J. (2015) A bitcoin technology gets Nasdaq test, *The Wall Street Journal*, May 10, 2015; Irrera, Anna (2015) CME and Deustche Börse Join Blockchain Gang, *Financial News*, July 20, 2015.

4 M-Pesa and BitPesa are mobile phone-based payment services. M-Pesa is not blockchain based, while BitPesa is. See http://www.coindesk.com/kenyan-court-upholds-bid-keep-bitpesa-off-mobile-money-platform/.

land registries onto blockchains, provide illustrations of the willingness of emerging economies to bypass older technologies and become early adopters of innovations that integrate economic data with information technology.

If blockchains attain a central role in corporate record-keeping, the maintenance and upgrading of blockchains themselves would raise interesting governance problems. Governance of a blockchain amounts to having authority to update its code, which might be done either for technical reasons or to change critical constraints or assumptions (such as the rate at which new coins or shares are issued). As implemented for bitcoin and other digital currencies, blockchains operate on a public, open, and decentralized basis, with all participants in a network (such as all owners of bitcoins) having the opportunity to update them in real time. Proposed changes to the Bitcoin blockchain code occur via a passive process of adoption or rejection by holders of more than 50% of the network's mining power, and in principle a change in the code can be initiated by anyone. As discussed in Section 4, this decentralization of authority over a blockchain might leave it vulnerable to sabotage. Rogue participants intent on crashing the network or diverting assets to themselves might propose software changes that appear benign and are widely adopted, or alternatively, might tempt others to adopt them using strategies based on the exploitation of collective action problems. Overcoming these vulnerabilities appears to be an important, unfinished priority for promoters of public blockchain technology in its open source form. The alternative of a permissioned blockchain, updated only by authorized participants, appears attractive for security reasons, but it would lack some of the appealing features of an open blockchain.[5] The most extreme alternative, a private blockchain controlled by a central gatekeeper authority, would concentrate operational risk in a single point of failure and might charge monopolist rents to network users or fail to treat them evenhandedly. Making such powerful third parties obselete and disintermediating financial transactions was the central goal of Nakamoto's (2008) proposal for a peer-to-peer electronic cash system.

The remainder of the essay is organized as follows. Section 2 provides a description of blockchains and how they function. Section 3 identifies and discusses a range of corporate governance arrangements that might be altered in a firm registering its securities on a blockchain. Section 4 discusses governance issues connected to the administration of blockchains. Section 5 concludes the paper.

2. How Blockchains Work

A blockchain records data in a sequential archive. Haber and Stornetta (1991) proposed this structure for time-stamping the creation of intellectual property, such as a digital document, in order to fix property rights with the creator before it can be copied by others. Haber and Stornetta's model assured the authenticity of each time stamp using hash functions, a type of cryptography that transforms data into a hexidecimal code of fixed length

5 The cost and benefit tradeoffs between public, permissioned, and private blockchains have become the basis of ongoing debates among industry players. See, for example, "Nick Szabo on 'Permissioned Blockchains' and the Block Size," available at https://bitcoinmagazine.com/articles/nick-szabo-permissioned-blockchains-block-size-1441833598, and "On Public and Private Blockchains," available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

which cannot be inverted to recover the original input.[6] The authors proposed transforming each entry in their sequence into a hash code, which would then be combined with the raw data for the next entry and turned into another hash code, which would then be added to raw data for the subsequent entry, *ad infinitum*. An archive of records in this form could authenticate the time of creation of any digital document by allowing users to match the document's hash code with the equivalent data embedded in the chain. Attempting to forge the information retroactively by changing a prior entry in the archive would cause changes in the sequence of all subsequent entries, since any minor alteration to the input of a hash function causes a significant change in its output that is trivial to observe.

A further component of Haber and Stornetta's scheme called for publishing the sequence of records in a public forum, such as a newspaper or a usenet post, where data could be verified by any interested user. This strategy, now known as a "distributed ledger," essentially crowd-sources the verification function classically played by auditors or bank inspectors, and it is an essential component of the open blockchain structure introduced by Nakamoto (2008) for Bitcoin. Nakamoto wrote that "[T]ransactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received."

Although the original design of Haber and Stornetta (1991) featured a sequence or "chain" of individual transaction entries, one item at a time, implementing the idea in very large markets with millions of assets required grouping many transactions together so that the need for computer memory remained reasonable. In subsequent work to develop the concept, they and other authors to proposed bundling large volumes of transactions together into "blocks" and arranging these blocks in chronological sequence using hash functions. Within each block, individual transactions would be condensed using a separate hierarchical system of hash pointers known as a Merkle tree.[7] Thus, Nakamoto's Bitcoin blockchain bundles together up to 1 MB volume of transactions culled from the network into a new block approximately every 10 min.[8] Blocks are "chained" together in the pattern proposed by Haber and Stornetta (1991), because the header of each block contains a hash function reflecting the contents of the previous block, which itself includes a hash function derived from its predecessor, and so forth, all the way back to the first block in the

6 The security of hash functions represents a critical component of not only blockchains, but also of much of modern Internet communication. In principle, a hash function could be inverted through trial-and-error, but an impractically large amount of time and computer hardware would be required.

7 Ralph Merkle, an American computer scientist, has been responsible since the 1970s for numerous breakthroughs in modern cryptography, many of them involving the secure creation of hash functions and the concatenation of hash functions within one another.

8 The 1 MB Bitcoin block size is an upper limit, and recently most blocks have clustered around 0.75B in size, containing approximately 1,500 transactions, with the average block size having increased steadily since 2009. On certain days, it is not unusual for most of the blocks to be full. During busy periods on the network, transactions not yet encoded into the blockchain sit in a buffer "memory pool." Nakamoto (2008) provides references to other cryptography papers that informed Bitcoin's design, and the author suggested the 10 min blockchain update interval based on an ad hoc forecast of future computer memory requirements. Today the growth of Bitcoin has led to vigorous user debates about optimal block sizes and cycle times, and rival digital currencies have proposed other parameters.

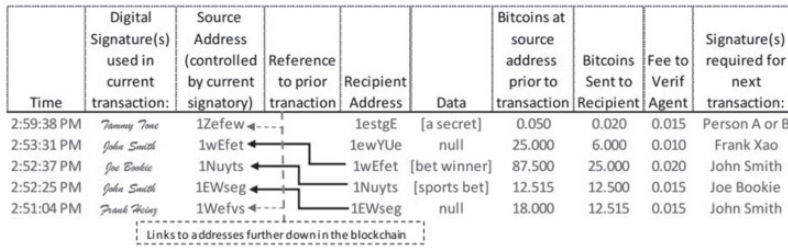

Figure 1. Transaction data in the Bitcoin public ledger.
The figure shows the types of data included in Bitcoin transactions, including the source and recipient, the amount of currency conveyed, and the time. The Data field can be used to convey additional information and is useful for "colored coins" applications as discussed in the text. The Fee to Verification Agent is an optional fee that the source can set aside for the miner who includes the transaction in a block.
Source: SolidX Partners, Inc.
Reproduced with permission.

chain. Figure 1 illustrates the type of data included in Bitcoin transactions, including the sender, recipient, amount, and time.

The party with authority to encode new transactions into a blockchain, who can be thought of as a sponsor or gatekeeper for the archive, holds enormous power that potentially poses great risks to individual blockchain participants. The gatekeeper can restrict entry into a market, assess monopolistic user fees, edit incoming data, treat some users preferentially, limit users' access to market data, and possibly share user data with outsiders, among other problems. In many of the prominent blockchain applications now under development, such as the Australian Securities Exchange in Sydney and the Depository Trust Clearing Corp. in New York, the gatekeeper role is assumed by an established "trusted third party" whose actions are constrained by government regulators as well as reputational considerations. A blockchain organized by a powerful sponsor of this type is often referred to as a "private" blockchain, since access for customers requires consent of the gatekeeper.

Motivated by distrust of the financial establishment,[9] Nakamoto (2008) introduced a blockchain design for Bitcoin with no sponsor or gatekeeper controlling the addition of new blocks. Instead, the update function was decentralized to all market participants in an ongoing competition catalyzed by the award of new bitcoins to the winner. As illustrated in

9 Nakamoto's lack of confidence in the mainstream banking system is evidenced by the "genesis block" of bitcoins created on January 3, 2009, into which he encoded the front page headline from that day's *Times* of London: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." Further, in a February 11, 2009, Internet posting, Nakamoto wrote: "The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts." See http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

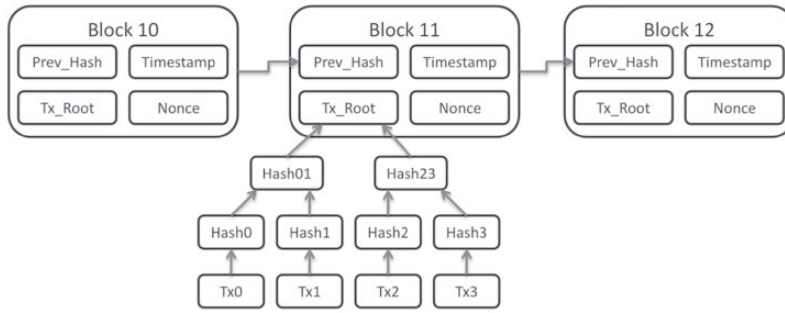

Figure 2. Structure of the bitcoin blockchain.
The figure shows the elements of each block on the Bitcoin blockchain, including transaction data, a timestamp, a nonce or random number related to the proof-of-work algorithm, and the hash of the header of the previous block. If any element of transaction data in a block is changed, the Tx_Root (or Merkle root) of the transaction data will change, causing the hash of the block header to change. Since the hash of the block header is included as an element in the header of the next block, the hash of the next block header will also change, as will the subsequent block headers, *ad infinitum*, thereby making fraud or theft easy to detect at the point at which it occurred.
Illustration: Matthäus Wander.
Reproduced under Creative Commons Attribution-ShareAlike License.
https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.png.

Figure 2, to create a new block in the Bitcoin blockchain, the operator of a "node" on the network must bundle together transaction data, the hash code from the header of the prior block, the time stamp, and a further piece of data known as a "nonce." The nonce is a random number with the property that, when added to the other information in a block, it generates a hash with a certain number of leading zeroes.[10] Once the fastest (or luckiest) miner finds a nonce and successfully completes a block with the required hash, network members will then verify and acknowledge the new block and begin working on its successor. A winning hash can only be discovered through trial-and-error, a computationally costly "proof of work" process that deters hackers from attempting to update the blockchain with fraudulent data.[11] Nakamoto observed that the award of new bitcoins to the first node discovering a rare hash "adds an incentive for nodes to support the network . . . [and] is analogous to gold miners expending resources to add gold to circulation," thereby leading these network members to become known as "miners."[12] Miners competing to create new blocks

10 In general, no two miners will bundle together the same set of transactions in the same sequence when attempting to create a block, so the nonce required to create a special hash and complete the block will be different for every miner.

11 Further security for the network comes from the requirement that each transaction be ratified by the sender using his or her "private key," similar to a password, which fits in a certain way with their "public key," similar to a virtual address. This double-key requirement prevents the creation of purely fictitious transactions by which a crooked miner might divert transactions to themselves.

12 Currently between 5,000 and 7,000 nodes take part in the Bitcoin network at any one time, and while all miners are nodes, not all nodes are miners. See www.reddit.com/r/BitcoinBeginners/comments/2rpmyl/what_is_the_difference_between_running_a_node_and/.

have discretion over which transactions to bundle, and no FIFO or other sequencing protocol is required.

Maintaining an equilibrium between the number of miners, the size of the mining reward, and the work required to create each new block, all while meeting the needs of the network, represents a complex balancing problem. The current reward to miners is 12.5 bitcoins per block. Approximately every 4 years the reward is cut in half, and recently it fell from 25 to 12.5 bitcoins in July 2016. Unless changed in the future, the reward will disappear altogether by 2140, at which point 21 million bitcoins will have been mined. After that, voluntary user fees from agents seeking fast verification of transactions (i.e., liquidity) will serve as incentives for miners to include them in their next blocks. This scheme follows the intent of Nakamoto (2008), who wrote that "Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free."

The Bitcoin network endogenously adjusts the difficulty of finding a winning hash by requiring either more or fewer leading zeroes in the hash of a new block; the difficulty changes periodically based on recent processing times so that new blocks require approximately 10 minutes of computational effort. In addition to making it costly for miners to create the next block in a blockchain, this method makes retroactive editing of the blockchain prohibitively difficult, since even a minor change in a past block would have the ripple effect of changing the hash codes of all subsequent blocks. A thief or forger seeking to alter old transactions would therefore face the insurmountable problem of having to find valid hashes for all subsequent block headers up to the latest, even as honest miners continued to work at extending the true blockchain. The difficulty of this task explains why commentators sometimes refer to information on a blockchain as "immutable" or "indelible."[13] Figure 3 illustrates the logic of the proof-of-work method in ensuring the integrity of historical data in a blockchain.

The decentralized mining protocol for extending an open blockchain, sometimes referred to as "competitive bookkeeping," has been incorporated into numerous other digital currencies and other public blockchain applications that permit open entry for anyone but require a method to discourage thieves and saboteurs. Along with sufficient incentives to obtain participation by miners, the protocol requires transparency of all blocks so that users have the opportunity to observe any data tampering that occurs. This open model of a blockchain, with no restrictions on entry, complete transparency of data, endogenous adjustment of proof-of-work incentives, and a passive system of governance, offers a sharp contrast to a private blockchain that limits access. One clear cost of the public blockchain model is the cost of the proof of work needed to update it, comprised of computer hardware and electricity. On the Bitcoin network, mining has become intensely competitive, and analyses of the cost of mining generally assume that capacity is added up to the point where the marginal cost of mining new blocks (aggregated across all miners) equals the market value of the expected reward in new bitcoins. At recent prices, if a block contains about 1,500 transactions, the mining reward

13 Any such claim of immutability ignores the possibility that a blockchain can be partly rewritten if a majority of the community supports a "hard fork," which occurred with Ethereum in the summer in 2016. In addition, a saboteur could compromise the integrity of the blockchain's data either by having a much faster supercomputer than anyone else or by adding enough CPU power to the network to control a majority of the mining power and organize a so-called "51% attack," a possibility discussed below.

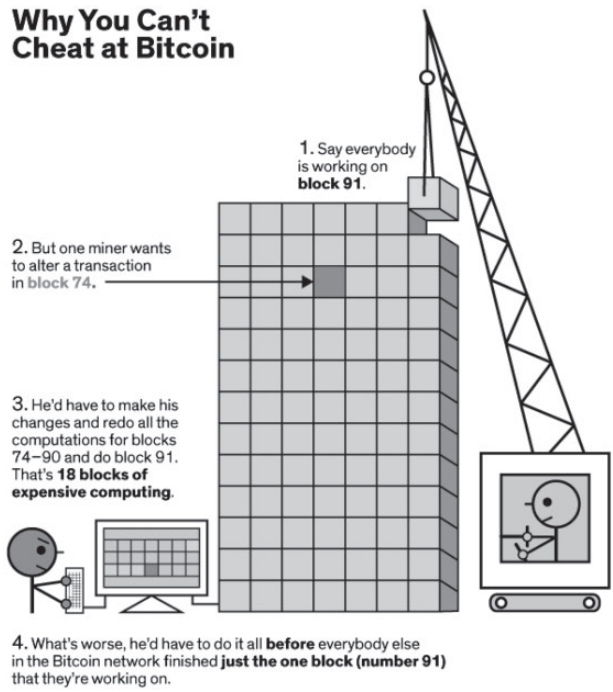

Figure 3. Integrity of data on a proof-of-work blockchain.
The figure illustrates how a proof-of-work scheme makes altering historical data in a blockchain prohibitively costly, since a potential thief or forger would have to alter not only the transaction record they wished to divert, but also all subsequent blocks up to the current one.
Illustration: Mark Montgomery © IEEE Spectrum.
Reproduced with permission.

is 12.5 bitcoins per block, and a bitcoin is worth about $725.00, then the current cost to validate each transaction should be in the neighborhood of $725.00 x 12.5/1,500 ≈ $6.00.[14]

In his conception of the Bitcoin blockchain as a distributed open source ledger, Nakamoto implemented an idea very similar to Kocherlakota's (1998) "money is memory" theory, although Nakamoto does not seem to have been aware of this economist's work. Kocherlakota reasons that agents treat money as a store of value because they believe that each owner of a coin obtained the money by delivering goods or services to the coin's prior owner, who in turn did the same with the predecessor owner. Kocherlakota's formal model

14 There are further sunk costs for expenditures such as the development of dedicated computer chips custom designed for bitcoin mining. Precise estimates of the Bitcoin network's power consumption are impossible to construct due to its ever-shifting capacity, but many stories in the news media have benchmarked it by comparisons with the energy demands of entire US states or small countries. See, for example, Izabella Kaminska, "Bitcoin's wasted power—and how it could be used to heat homes," *Financial Times*, September 5, 2014. These estimates seem misleading, however, because bitcoin miners tend to cluster in areas where electric power is cheap and abundant and might otherwise go unused. The best known locations include Iceland, which has access to geothermal power, and Inner Mongolia, which has abundant hydroelectric power.

shows that any economic allocation achieved through the use of money could be replicated if all agents knew the complete history of everyone's exchanges and kept a running account of their net contributions to the economy, using each agent's net economic surplus earned as a signal of their claim against other agents with net deficits. Nakamoto wrote that "We define an electronic coin as a chain of digital signatures." In other words, each bitcoin is made valuable by the ability to attach to it the memory of its previous exchanges.

The Bitcoin blockchain has proven to be stable through more than 7 years of continuous use, and its reliability has led many developers of blockchain products to propose free-riding upon the Bitcoin network through a strategy known as "colored coins." To transfer an asset, such as a share of stock, one could initiate a bitcoin transfer from the seller to the buyer involving a trivial amount of bitcoins, such as 0.00001. Attached to this transaction in an additional data field could be a "token" such as the share of stock (see the Data field in Figure 1). Miners would then bundle up the transaction into the next block, and the record of the bitcoin transfer would also serve as proof of transfer of the stock. Although this strategy seems appealing because it saves development cost and takes advantage of Bitcoin's reliability, it raises a number of legal and enforcement issues since the Bitcoin network was designed to transmit only bitcoins themselves and may not be suited to the special characteristics of other assets. These issues are explored in a recent paper by Swanson (2015). Alternatively, a company could sponsor its own blockchain and either update the blockchain itself or establish an incentive system attract miners from outside.[15]

Refinements and appendages to public and private blockchains are quickly emerging. A "permissioned" blockchain restricts updating privileges to a select group of authorized users who negotiate governance and control rights among themselves, in a process loosely resembling a partnership agreement. Permissioned blockchains offer clear advantages in security and privacy while potentially reducing costs of compliance with regulations such as "know your customer" money laundering regulation in the USA. Many of the most prominent blockchain organizations, such as Hyperledger and R3CEV, have followed this model. In a "sidechain" (Back *et al.*, 2014) a sponsor can operate a private or permissioned ledger but periodically connect some aggregation of its transactions to an open, distributed ledger, or two private ledgers could exchange transaction data in both directions. Sidechains offer potential benefits such as the ability to accommodate overflow transaction volume that may exhaust the throughput capacity of the main blockchain. Other platforms such as Ethereum incorporate many features of blockchains while adding additional functionality, such as a contracting language that allows users to establish contingencies for the transfer of assets and to reach out to an agreed-upon oracle to arbitrate disputes.

For the interested reader, Bheemaiah (2015) provides an easily accessible discussion of the important technical details, and The Economist (2015) offers a very useful general

15 One could imagine a company autonomously issuing shares of its stock on an open blockchain that is updated by miners on a decentralized basis. Miners could receive a modest allocation of new shares as a reward (diluting the old shareholders, as with bitcoin's blockchain), or the blockchain could require stock traders to include user fees for each transaction. Of course, the company could also operate a private blockchain that it updated itself. The first known case of this came to light in November 2016 when Overstock.com began taking subscriptions for an equity rights issue over a private blockchain. See http://www.coindesk.com/overstock-raise-30-million-blockchain-stock-offering/.

introduction and characterizes the blockchain as a "trust machine," since its algorithms report economic transactions with very high precision without any need for a trusted third party. Böhme *et al.* (2015) provide a survey of the Bitcoin network and a lucid discussion of its underlying principles and governance and the range of potential future applications.

3. Corporate Governance of Firms Traded on Blockchains

Issuing and trading corporate securities on blockchains would create numerous benefits and also certain costs related to greater transparency of ownership and faster, cheaper trade execution and settlement. Better transparency would significantly impact the profit opportunities available to managers, institutional investors, and shareholder activists, among others, because the incentives to acquire ownership and to liquidate it could change markedly if their transactions were observable in real time. Improvements in trading technology would also affect the incentives to acquire and liquidate ownership for these groups. Important side effects might spill over into the real economy, since the changing incentives for informed investors to trade might lead to more reliable signals about the value of individual firms. In the presence of these changes, over time suppliers of capital might design securities differently, reconsidering the need for certain restrictive covenants and taking advantage of blockchains' ability to execute "smart contracts" autonomously. Firms may recruit board members and outside consultants with different skill sets to deal with these changes, and important topics like management incentives would likely evolve to take account of the changing nature of corporate securities.

3.1 Greater Transparency of Ownership

When used in an open form with free entry and exit, blockchains generate an archive of transactions known as a distributed ledger, because a copy of each block of transactions is distributed or made visible to all members of the network. The original Haber and Stornetta (1991) paper, in which the blockchain structure was proposed for authenticating intellectual property, suggested this structure to crowdsource the function of auditing and verification. For a company with shares listed on a public blockchain, all shareholders and other interested parties would be able to view the arrangement of ownership at any time and identify changes instantly as they occurred.

Not all shareholders would be attracted to this arrangement; activists, raiders, or managers might wish to conceal their trades for exactly the same reasons that small shareholders or fund managers might wish to observe them. Firms issuing equity would have to balance these considerations and evaluate whether marketing their shares would be more lucrative on a private or permissioned blockchain, where the visibility of transactions could be restricted to a set of member firms or trusted gatekeepers and investors would enjoy more anonymity. Even under the private or permissioned blockchain models, the real-time archive of transactions would create much more current and complete information about each firm's ownership than is available in stock markets today, and it would be visible to at least some observers. If the ledger of transactions were visible only to the blockchain sponsor and to the government, the impact on investors' trading strategies and insiders' incentives could still be profound as discussed below. Ultimately, a range of blockchains offering varying degrees of investor anonymity might compete in the market to attract corporate listings, with companies sorting themselves among different platforms that appealed to different shareholder clienteles based on their preferences for ownership transparency.

Ironically, issuing companies might find public blockchains attractive as a type of takeover defense, because their transparent structure undercuts the secrecy prized by shareholder activists and corporate raiders when building hostile positions and instead promotes passive shareholder behavior in line with the Grossman and Hart (1980) free-rider problem.

All of these conjectures assume that those able to view the distributed ledger of share ownership would be able to identify the holders of individual shares and the counterparties of important transactions. For instance, if a manager sold shares of his own stock, I assume that others will not only observe the sale but will also discern the selling manager's identity. In practice, this may or may not occur, because assets on blockchains are typically held in anonymous "digital wallets" identified only by complex labels akin to serial numbers. Many early users of bitcoin were attracted to the currency precisely for this reason, because they believed the blockchain provided anonymity for purchases of drugs, money laundering, and other illegal activities.

How easily the identity of a party transacting on a blockchain could be identified is a matter of debate, and authors such as Malinova and Park (2016) argue that mandatory disclosure of traders' identifying codes would be welfare increasing for the market as a whole. One would expect the demand for identification of ownership on a blockchain to lead to a growth in specialist "de-anonymizing" research firms that already exist, earning subscriber fees by ascertaining the ownership of individual digital wallet addresses. This process amounts to a modernization of the de-coding methods that Wall Street participants have used for decades if not centuries, attempting to infer the presence of certain buyers or sellers in the market by observing details of the size, timing, and sequence of their trades.

On the Bitcoin blockchain, maintaining anonymity has at times proven difficult. Law enforcement officials have successfully identified and prosecuted money launderers, drug dealers, operators of virtual casinos and Ponzi schemes, and other miscreants. If a company issued equity on a public blockchain resembling bitcoin's, the situation would probably be similar. Even without advanced forensics, one could rather easily match digital wallets with individual stock traders by searching the raw data for a particular transaction pattern that is known to have occurred, such as a company's award to a manager of a certain quantity of restricted shares on a particular date. Potentially a share owner could stay a step ahead by using a different digital wallet for each transaction or breaking transactions into small pieces using several wallets at once. To defeat these strategies, regulators might require corporate insiders to disclose their digital wallet identifications, or public keys, under penalty of law. This would likely be part of an evolution of the disclosure regulations that most countries apply to managers and significant outside shareholders, who typically must identify themselves after passing certain ownership thresholds. Such notices to the market, such as the Schedule 13D filing for 5% activist shareholders in the USA, might become superfluous if these investors' positions could be observed in real time.[16]

16 Current US law provides for a deadline of 10 business days for an activist shareholder to file Schedule 13D, but the rule is currently under review by the Securities and Exchange Commission. In the USA, a patchwork of different disclosure rules applies to corporate insiders and outside institutions and activists (see Hu and Black, 2006, Table 3). Many of these rules were written years ago at a time when stock market transactions involved the movement of paper stock certificates and documents were filed by mail. Blockchain trading platforms might eventually lead regulators to reconsider whether these rules were still necessary or how much time different investors should be given to comply with them.

3.2 Improvements in Liquidity

According to a recent survey by Holden, Jacobsen, and Subrahmanyam (2013), liquidity is "the ability to trade a significant quantity of a security at a low cost in a short time." Due to their potential to reduce costs and shorten the time required for executing and settling securities trades, blockchains offer the possibility of significant improvements in liquidity, whether they are used as the main platform for share registration and exchange, or alternatively, whether they are introduced by stock markets in a more limited way to streamline the post-trade clearing and settlement process.

Stock trades in the USA generally require three business days for settlement to occur and ownership to move formally from seller to buyer. During this interval, funds pass between brokers and their clients, and shares are transferred on the books of the brokerage and the ledger of the corporation, all under the supervision of the Depository Trust Clearing Corp. Many people are involved in this process. In contrast, a sale of stock on the blockchain could be settled much more quickly, depending upon the cycle time for adding new blocks, and it would not require numerous middlemen, reducing the costs that now appear variously in commissions and bid-ask spreads. Although stock markets would probably continue to operate in some form to facilitate the meeting of buyers and sellers, liquidity could increase greatly in response to the lower cost and faster speed of settlement. Cost savings on a blockchain market would take both direct and indirect forms. The direct cost savings would accrue from the reduction in personnel and streamlining of processes compared with those used currently. Indirect savings, potentially larger, would emerge from the reduced need for firms to tie up assets in collateral as a form of bonding during the settlement process.[17]

Liquidity is a critical issue for portfolio managers and other investors both large and small. Improving liquidity could increase the demand for stocks and have many significant effects on patterns of investment and ownership. For instance, high frequency equity trading might become much more common if the cost of trading were reduced through this type of innovation.

3.3 Impact on Institutional Investors and Activists

Major outside shareholders would be affected by both the greater transparency and improved liquidity that could arise from blockchains. As shown in a survey by Edmans (2014), a large number of papers have studied the impact upon shareholder activism of either or both of these forces, and certain models predict either greater or lesser involvement by major shareholders in corporate governance when either transparency or liquidity is increased.

Greater transparency would potentially be seen as costly by activists and raiders, and as a result they might be more reluctant to invest in firms that were traded in blockchain markets. Building share positions secretly is a time-honored strategy of these investors, who wish to minimize their costs of acquisition by avoiding publicity as they buy (Bebchuk and

17 One major bank official states, "An interesting application of this could be around enhancing the velocity of movement of securities, enabling financial institutions to mobilise collateral to back up their trades more quickly ... Collateral management is a critical topic now." See Jon Watkins, "Could the Blockchain solve the collateral conundrum?" The Trade, October 6, 2015, available at http://www.thetradenews.com/Asset-Classes/Derivatives/Could-the-Blockchain-solve-the-collateral-conundrum-/.

Jackson, 2012). Many of these investors also wish to control the timing of their self-identification in order to take corporate managers by surprise for tactical reasons. Assuming that the market could identify activists as the buyers of shares—which might be apparent due to the large size or well-known patterns of their purchases—then shareholder activism might become more costly and less prevalent for firms with blockchain share trading. See the models in Kyle and Vila (1991) and Collin-Dufresne and Fos (2016), as well as the data in Collin-Dufresne and Fos (2015), showing that blockholders' trades are highly profitable during the period before they are required to disclose their ownership positions.

However, models with the opposite implication appear in Maug (1998) and Kahn and Winton (1998); these papers suggest that transparency helps major shareholders by improving liquidity and lowering their costs. This effect occurs because once the large shareholder's presence is disclosed, other shareholders expect them to become well informed and would wish to sell their shares quickly rather than risk trading at an informational disadvantage in the future.

The impact of greater liquidity upon institutional investors and shareholder activists seems likely to be complex. In a blockchain market, cheaper and faster trade execution and settlement would facilitate both easier entry and easier exit by major shareholders. The greater ease of entry would probably promote ownership by institutions and activists. Edmans, Fang, and Zur (2013) is one of many papers showing the benefits of greater liquidity to large outside stockholders who seek to involve themselves a firm's management. Norli, Ostergaard, and Schindele (2015) show that activists accumulate more shares when liquidity is greater.

Once investors have purchased their position, they can choose to influence a firm's management through the threat of sale, or exit, or through negotiation and participation in corporate voting, or voice. A rich literature has analyzed both of these channels, and, *ceteris paribus*, the increased liquidity of a blockchain market should reduce the costs of selling and therefore lead to more emphasis on exit as opposed to voice. For example, in Edmans's (2009) model, liquidity increases the credibility of a blockholder's threat to sell, helping blockholders induce managers to improve project selection. Admati and Pfleiderer (2009) present a model in which the threat of exit deters managers from accepting non-value maximizing projects that have private benefits. Rosenbloom, Schlingemann, and Vasconcelos (2014) find that bidder returns in mergers are higher when the bidder's own stock liquidity is lower, which raises the cost of exit for institutional investors and gives them indirect motivation to use voice to restrain managers from pursuing bad acquisitions.

3.4 Impact on Managers

Blockchain trading of a company's shares would likely reduce the effectiveness of equity-based management incentives.

Corporate managers obtain most of their incentives from stock compensation, either from stock options or restricted shares. Insider trading regulations constrain managers' ability to profit from trades in their own shares. However, an influential literature argues that even when managers trade within the established legal boundaries, insider trading represents a *de facto* compensation system for them, allowing executives to exploit at least a certain amount of inside information and reap some of the profit associated with the valuable news they create. See Baiman and Verrecchia (1996) and Roulstone (2003), who provides an explanation, rooted in the theories of Manne (1966), for why insider trading,

whether legal or illegal, may represent an effective incentive system that alings managers' and shareholders' interests.

Blockchain share trading would potentially allow outsiders to observe managers' trades in real time. Investors are keenly interested in knowing when managers receive or liquidate equity in their own firms, both because any transaction changes the managers' incentives, and because managers' transactions likely signal private information about the firm.[18] Real-time transparency of trading would expose managers to greater scrutiny by their boards and shareholders, probably causing them to trade less often out of concern of sending adverse signals to the market. The net effect would likely cut into managers' profits from legal insider trading, and firms might have to pay them more to offset this loss. At the same time, the managers would have diminished incentives to create valuable information that they might be able to exploit via insider trading, potentially reducing their alignment with shareholders.

A related problem for managers would be greater market awareness of when their shares were pledged as collateral for loans or in connection with derivative hedging products (Bettis, Bizjak, and Kalpathy, 2015). These strategies are often used by managers to achieve *de facto* liquidation of their equity incentives without incurring tax or signaling costs. In a blockchain registration system, a pledge of shares would probably be visible as a type of contingent smart contract, and managers might incur various tax or reputational penalties that they can currently avoid due to the opaqueness of these transactions under today's regulatory system.

A blockchain registration system would also preclude managers' backdating of compensation instruments. Over the past decade, research has shown that managers obtain financial profits and tax benefits through the backdating, variously, of stock option awards (Heron and Lie, 2007), stock option exercises (Cicero, 2009), and charitable gifts of stock (Yermack, 2009). Blockchains are add-only databases in which entries are time-stamped and cannot be rewritten once entered. Therefore, share transfers could not be backdated or otherwise changed retroactively, a reform that outside shareholders might view as value-improving even while managers would see it as costly.

The transparency afforded by a blockchain system would illuminate managers' ownership positions not only in their own firms, but also in other companies' shares, including those of competitor firms. This visibility could strengthen relative performance evaluation systems. Many compensation reform proposals have argued for relative performance evaluation, in which a manager is awarded equity pay that is benchmarked against a market or industry index. These schemes essentially give the manager a short position in the benchmark index, but the manager can offset such a contract by privately taking a long position in the same benchmark. For instance, an executive of Coca Cola whose share price performance is being compared against that of Pepsi could covertly take a long position in Pepsi. Ordinarily, trading in shares of a competitor is not visible to the board of directors or to regulators, since it lies beyond the boundaries of insider trading disclosure requirements. We have no knowledge

18 One of the most significant aspects of the 2002 Sarbanes–Oxley Act in the USA was a reduction in the required filing period for managers following their acquisitions and dispositions of shares. The previous rule, which required paper filing by the tenth day of the subsequent calendar month, was changed to require electronic disclosure within two business days. As shown by Brochet (2010), the market reacted more significantly to announcements of managers' transactions once the more timely reporting requirements took effect.

of how often managers engage in such trades to weaken relative performance incentives that their boards seek to impose upon them. Of course, if boards could view these trades and restrict them, the managers' welfare would decrease, and firms might have to pay them increased compensation to meet their reservation utility levels.

3.5 Impact on Market Microstructure

The potential microstructure implications of a blockchain share market are vast, and a thorough study of these possibilities is beyond the scope of this paper. In this subsection, I outline a few of the immediately clear predictions about possible changes in market trading, price formation, and the mix of information impounded into share prices.

In today's markets, if traders' identities are opaque, then distinguishing informed traders from noise traders or liquidity traders can be difficult for market makers. This is especially true when an investor is selling, since many sales occur due to liquidity shocks whereas purchases are more likely to be driven by informational advantages, since positive liquidity shocks are far less frequent than negative ones. Brochet (2010) and other studies therefore find that managers' trades receive much stronger market reactions when they are purchases rather than sales. If blockchains improve the transparency of investor identities, then informed selling could become easier to differentiate than before, and the speed with which adverse news is impounded into share prices could therefore increase. This would represent a change from current market patterns, in which good news generally reaches the market more readily than bad news (see, e.g., Hong, Lim, and Stein, 2000).

The increased transparency of a blockchain share registration system could permit market makers to observe investors' ownership positions not only in the shares they are transacting, but in other shares as well. Following the logic of Edmans, Levit, and Reilly (2016), consider an investor who owns two stocks, with each traded by a separate market maker who cannot observe the trade in the other share. If the investor sells, the market maker may consider the trade to be based either upon adverse information or a liquidity shock. The ability to observe whether the investor sells the other share at the same time would improve the precision of the market maker's inferences about whether individual trades are information driven or liquidity driven. This could potentially lead to more efficient prices and reduced risk premiums charged by the market maker. More informative prices would in turn improve the allocative efficiency of the real economy by enabling managers, investors, suppliers, and others to make better decisions about the price and volume of capital allocated to different firms and projects.

If the greater transparency of blockchains deterred insider trading by managers, as argued above, outside investors and analysts would have greater incentives to invest in acquiring information about the firm. See Fishman and Hagerty (1992) and Bushman, Piotroski, and Smith (2005). This could rearrange the overall distribution of information in the economy and potentially lead to greater allocative efficiency of outside investment. See Leland (1992), who discusses the implications of legalizing insider trading for capital investment, market liquidity, and the welfare of outside investors. The greater liquidity afforded by blockchains could increase the incentives of analysts and investors to gather private information, since they could more readily obtain a benefit from the information. This effect would have governance implications by improving the outside monitoring of management.

3.6 Voting in Corporate Elections

Blockchain technology has been proposed as a platform for voting in all types of elections (Boucher, 2016),[19] and it appears to be a viable substitute for the archaic corporate proxy voting system that has endured for hundreds of years with surprisingly few concessions to modern technology. In February 2016, the NASDAQ Talinn (Estonia) Stock Exchange announced a pilot program for blockchain voting in shareholder meetings for companies listed on the exchange. The NASDAQ, which is the corporate parent of a much larger stock exchange in New York, stated in its announcement that "blockchain technology will allow votes to be quickly and securely recorded, streamlining a proxy voting process that has historically been labor-intensive and fragmented."

Many studies such as Kahan and Rock (2008) have documented the current problems with corporate elections, which include inexact voter lists, incomplete distribution of ballots, and sometimes chaotic vote tabulation. In a blockchain election, eligible voters would receive tokens (sometimes called "votecoins") that they could transmit to addresses on the blockchain to register their preferences. As discussed by Wright and DeFilippi (2015), the greater speed, transparency, and accuracy of blockchain voting could motivate shareholders to participate more directly in corporate governance and demand votes on more topics and with greater frequency.[20] Due to the transparency of blockchains, ensuring the anonymity of voters would be an obvious problem, but this problem would be confined to a minority of companies since most corporations currently do not use confidential voting.

3.6.a. Accuracy of elections

The imprecision of vote tabulation under currently used procedures implies a high degree of inaccuracy in the outcome of close corporate elections. One Delaware attorney "estimates that, in a contest that is closer than 55 to 45%, there is no verifiable answer to the question, 'who won?'"[21] The vagaries of vote tabulation, such as when the polls actually close and whether all the votes are counted, seem to introduce noise. In addition, Listokin (2008) presents results showing that close elections end up being decided in favor of management in a disproportionate number of cases, implying that the results are subject to manipulation. He writes that, "at some point in the voting process, management obtains highly accurate information about the likely voting outcome and, based on that information, acts to influence the vote," although the mechanisms used by management, such as last-minute lobbying of dissident voters, are not clear.

The benefits of blockchain elections would include faster, more precise vote tabulation, and equal real-time transparency of the likely voting outcome for both management and dissident shareholders. This could give each side an equal opportunity to intervene with last-minute campaign tactics and resolve ambiguities about the outcomes of close elections. The net effect could be more frequent election of dissident outside candidates representing shareholder activists or other groups and potentially more frequent defeats of management proposals related to compensation and governance.

19 See www.v-initiative.org for a well-known example.

20 In 2015 Broadridge Financial Services, which tabulates votes in most US corporate elections, reported voter turnout rates of 83% for institutional investors but only 28% for household retail investors, with much smaller rates for micro cap stocks. See http://media.broadridge.com/documents/Broadridge-PwC-ProxyPulse-1st-Edition-2015.pdf.

21 Kahan and Rock (2008, p. 1279).

3.6.b. Empty voting

Empty voting occurs when an investor uses borrowed shares or certain combinations of derivative securities to acquire voting rights temporarily, without economic exposure to the cash flow rights connected to the underlying shares. Hu and Black (2006) and Christoffersen *et al.* (2007) describe empty voting in detail. Many of these strategies rely on secrecy and can culminate in investors appearing on election day with far more votes than expected. Some empty voting schemes are not strictly legal but have succeeded due to the difficulties of observation and enforcement.

Empty voting is controversial. Opponents tend to label it as undemocratic, since it involves acquiring voting rights separate from the other antecedents of ownership and may potentially be used to vote for the "wrong" side of a ballot question in order to create adverse outcomes that somehow benefit the empty voter. However, supporters view empty voting as efficient, since it permits voting rights to be priced according to their marginal benefit to the highest-valued voter, and it provides an opportunity for minority shareholders to profit by selling (or temporarily renting out) their votes. See Brav and Matthews (2011). Whatever the merits of these arguments, it seems plain that empty voting would become more difficult under blockchain share registration, which would provide both transparency and early warning of the rearrangement of voting rights prior to an election. For example, the simplest type of empty voting involves borrowing shares in the stock lending market, with voting rights passing to the borrower until he returns the shares. Such a stock loan would be immediately transparent, providing notice to shareholders, management, and regulators of a redistribution of voting power. Opponents could take steps to counteract the acquisition of votes by an empty voter, and regulators could potentially enjoin voting of the shares.

3.7 Real-Time Accounting

Lazanis (2015) suggests that a firm could voluntarily post all of its ordinary business transactions on a public blockchain. This would occur automatically if the firm used digital currency as its medium of exchange, since the currency itself would reside on a blockchain, but it could also be done by means of tokenization, as discussed earlier, or even in conventional currency if done on a permissioned blockchain. Like all blockchain transactions, the firm's routine accounting data could be recorded permanently with a time stamp, preventing it from being altered ex-post. The company's entire ledger would then be visible immediately to any shareholder, customer, lender, trade creditor, or other interested party. Anyone could aggregate the firm's transactions into the form of an income statement and balance sheet at any time, and they would no longer need to rely on quarterly financial statements prepared by the firm and its auditors. Although this radical change in financial reporting would obviously come at a cost—making proprietary information available to outsiders—it would have two enormous benefits. Shareholders would have increased trust in the integrity of the company's data, and costly auditors (who are themselves corruptible) would not need to be hired to vouch for the accuracy of the company's books and records.

3.7.a. Accountants and financial intermediaries

In a world with real-time accounting, consumers of financial statement information would not need to rely on the judgment of auditors and the integrity of managers. Instead, they could trust with certainty the data on the blockchain and impose their own accounting judgment to make their own non-cash adjustments such as depreciation or inventory

revaluation. The potential US savings equals the total revenue of the accounting industry, which exceeds $50 billion per year. This sum represents the social cost for third-party validation of the accuracy of company accounts, or more simply, the social cost of mistrust of corporate managers. Instead of relying on the auditing industry, which itself has been subject to moral hazard and agency problems (Cunningham, 2006; Ronen, 2010), each user could costlessly create their own financial statements from the blockchain's data, for whatever time period they wished. Users could access the firm's raw data and make their own decisions about depreciation schedules, marking assets to fair market value, and recognizing non-cash accruals to earnings. To survive, accountants would need to reinvent themselves as interpreters of raw financial data, and given the large size and complexity of many companies, market demand for their services would probably continue in some form.

3.7.b. Accruals earnings management

Real-time accounting on the blockchain would greatly reduce opportunities for firms to engage in accounting gimmicks and value-destroying real actions to manipulate reported earnings. With irreversible, time-stamped transactions, managers could not use strategies such as backdating sales contracts to a prior reporting period or amortizing operating expenses, which should be expensed immediately, and pushing them into future periods. If users relied on their own custom financial statements, today's common reporting data and frequencies, such as quarterly earnings per share, might become much less important and therefore would be less frequently manipulated by managers. Security analysts would need to work harder to assess the fair values of company stocks, but they would have much more information with which to accomplish this task.

The potential implications of these changes are important, as executives may manage their firms differently if accruals earnings management became more difficult. Survey research indicates that managers are willing to make suboptimal investment decisions such as cutting positive NPV investments for the benefit of short-term gains in accounting earnings (Graham, Harvey, and Rajgopal, 2006).[22] If manipulation of quarterly earnings became much less important due to real-time accounting, perhaps this distortion in firms' investment policies would recede. However, the response by managers may not be simple to predict. Cohen, Dey, and Lys (2008) find a shift from accruals earnings management to real earnings management after the 2002 inception of the Sarbanes–Oxley Act, which restricted certain channels of accounting earnings management via discretionary accruals.

3.7.c. Related party transactions

Real-time accounting on the blockchain could allow observers instantly to spot suspicious asset transfers and other transactions that imply conflicts of interest. The disclosure rules of the USA and many other countries place a burden upon management to self-report these so-called related party transactions, but compliance is widely believed to be incomplete, and it is often subject to nuanced debates about which transactions are material enough to require disclosure. Transparency in this area would impact managerial incentives, since

22 Similarly, the introduction of quarterly earnings reporting in the European Union appears to have led to firms reducing long-term investments, improving short-term earnings at the expense of long-term earnings, according to the findings of Ernstberger *et al.* (2016). Kraft, Vashishtha, and Venkatachalam (2016) find a similar historical pattern in the USA, but Nallareddy, Pozen, and Rajgopal (2016) find no such pattern in the UK.

insiders would have less ability to tunnel assets out of the firm, and it would permit creditors to engage in real-time surveillance against fraudulent conveyances by managers of financially distressed firms. It could also add more costs for firms, if they had to explain large numbers of individual transactions to the public.

3.8. Smart Contracts

According to Szabo (1994), "a smart contract is a computerized protocol that executes the terms of a contract." Based on the same logic as a mechanical coke machine, a smart contract is designed to assure one party that the counterparty will fulfill his promises with certainty. Smart contracts can overcome moral hazard problems such as strategic default, and they can dramatically reduce costs of verification and enforcement (indeed, lawyers might see their business shrink dramatically in a world in which many contracts became self-enforcing). A number of new platforms such as Ethereum are designed to apply blockchain technology to execute smart contracts based on simple events such as the passage of time or complicated contingencies such as future financial outcomes.

Although smart contracts raise a number of difficult legal and enforcement issues, they have numerous potential applications in corporate finance and governance. These include the mechanical exercise of options embedded in derivative securities and other contingent claims, the instant transfer of collateral in the event of default, and the payment of employee compensation if performance goals are achieved, among many others. In many of these settings, smart contracts seem like a promising device for reducing agency costs. The willingness of a firm to enter into a smart contract could represent a precommitment not to behave opportunistically in the future, and it would protect a lender against basic fraud strategies by a debtor such as pledging the same collateral to two borrowers.

Smart contracts may not impact corporate governance directly in the way that blockchain stock training would. However, they could create significant long-term effects by deterring widely known agency costs of debt such as risk shifting and strategic default. This would have beneficial effects such as reduced adverse selection in credit markets and a lower cost of debt market-wide. Boards of directors might reconsider the need for banker-directors, who have classically filled a bonding role by signaling to the market that the firm is creditworthy (Sisli Ciamarra, 2012). Debt contracts might have fewer covenants, and the role of credit rating agencies could greatly diminish in importance.

4. Governance of Blockchains

Participants in blockchains—such as the companies who may list their shares on a blockchain stock registry—have many reasons to care about governance of a blockchain itself. An open public blockchain is operated autonomously by computer software (more specifically, by large numbers of miners who run the open source code). This code specifies basic inputs for each transaction, the timing and priority for encoding these transactions into the blockchain, and limits on the sizes or contingencies associated with each transaction, among other issues. These software parameters are akin to the rules and regulations of a stock exchange in which firms agree to list their shares and have them traded by third parties subject agreed-upon constraints and limitations.

Just as with a stock exchange's day-to-day rules, the regulations embedded in a blockchain's software code could favor some participating companies at the expense of others, and therefore the authority to change these underlying rules could become critically important. Ultimately blockchains must rely on a governance process in which the users agree upon a set of requirements for the underlying software code to be changed, including provisions for dispute resolution, sanctions for violating the agreed upon rules, and procedures for enforcement of penalties.[23] In a private or permissioned blockchain, negotiating these rules, including withdrawal rights, should be similar to the negotiation of a partnership agreement. In a public blockchain that can be joined by anyone, governance can become much more complicated.

What could go wrong to provoke a governance crisis among the users of an open blockchain in which transactions are validated on a proof-of-work basis? The most basic problem would be a so-called 51% attack, in which one participant on the blockchain controlled enough mining power in order to force through a change in the software to benefit themselves at the expense of everyone else. Acquiring this much capacity might be expensive, however, so one could imagine other, more subtle strategies.[24] For example, a saboteur could mislead network members into loading a new, faulty version of the code by misrepresenting its true capabilities. One could also tempt other nodes with a prisoner's dilemma type strategy, offering them modest payments that they will rationally accept in exchange for uploading the new, inferior software, even though abandonment of the old code makes the rest of the community worse off. Other divide-and-conquer strategies, using game theoretic analysis as the foundation, could also be devised. Protecting against these types of governance attacks may emerge as a significant problem for open source blockchains, and the issue does not seem to have received much attention from Nakamoto (2008) and other creators of the Bitcoin blockchain.[25] Even though Nakamoto's original paper raised concerns about the possibility of attacks against "honest nodes" by potential saboteurs, it does not consider the possibility of collusion among miners in a mining pool, something recognized as a clear potential danger today.

By far the most widely used, the Bitcoin blockchain is governed in an extremely decentralized way. The software code for Bitcoin is open source, and any user may propose a change to the code at any time. For a change to take effect, "consensus" is required, and it is manifested when more than 50% of the miners on the network have discarded the old code and begun running the new one. The procedure is purely passive and cumulative, with no particular election or decision point scheduled for users to evaluate the new code, and it is generally not time-limited unless the proponent of the new code introduces it with a contingency hard-coded in advance. Proposed changes to the code can simply be met with

23 An excellent example would be the US blockchain firm R3, which has organized a consortium of approximately 70 leading financial institutions to develop numerous platforms for trading assets using a distributed ledger system. It seems highly unlikely that all the institutions will agree upon the need and form of future modifications to their trading protocols, and they will need to work with R3 to establish governance procedures for these situations.

24 Mining pools have formed on a voluntary basis on the Bitcoin network to share the costs and mutualize the rewards of their work. In 2014 one pool, GHash.io, briefly exceeded 51% of the network power and was theoretically in a position to attack the network. The size of the pool created so much public controversy that some miners dropped out in order to shrink it.

25 See the blog posting by Tim Swanson at http://www.ofnumbers.com/2015/11/05/creative-angles-of-attacking-proof-of-work-blockchains/.

indifference and ignored, while others may emerge as the byproduct of high-profile discussions in online forums among expert participants in the network. Metz (2015) provides a good introduction to this process and discusses the current controversy within the Bitcoin community over whether to increase the sizes of blocks in the Bitcoin blockchain in order to accommodate higher transaction volume in real time. Although many agree on the need for changes to Bitcoin to handle increasing transaction volumes, numerous miners instead see a benefit to rationing the currently limited capacity, and several high-profile efforts to obtain consensus for reform have failed up to now.

An important event in 2016 highlighted the problems that can arise due to the uncertainties of blockchain governance. A successful hack occurred against the Ethereum platform, an open blockchain, in which the hackers diverted approximately $50 million worth of ether tokens from a decentralized autonomous organization known as the DAO. In response, the sponsors of Ethereum erased their blockchain from the point of the hack forward by implementing a "hard fork," thereby negating the theft by the hacker. This action, which was supported by 85% of the Ethereum miners, accomplished two things that were supposed to be impossible on a public blockchain: rewriting the history of transactions, and introducing human intervention to negate the unanticipated consequences of a self-executing smart contract. Implicitly, the event raised the possibility of future interventions into Bitcoin and other blockchains, even open ones, if a majority of the constituents wished to nullify a set of adverse economic outcomes after the fact. A minority of 15% of the Ethereum miners saw this precedent as dangerous and opposed the hard fork, creating a schism in Ethereum when they continued to mine and process transactions on the legacy blockchain, which they renamed "Ethereum Classic."

5. Conclusions

Blockchain technology offers a novel method for trading and tracking the ownership of financial assets. It appears to be a leap forward in financial record-keeping not seen since the introduction of double-entry bookkeeping centuries ago. Stock exchanges around the world have begun to experiment with blockchains as a method for companies to list, trade, and vote their shares, and stockholders may benefit from lower costs of trading, faster transfers of ownership, more accurate records, and greater transparency of the entire process.

Corporate governance could change in many ways under a blockchain regime. Institutional investors, raiders, and activists could benefit from being able to purchase shares at lower cost and to sell them into a market with greater liquidity, but they would have a much more difficult time disguising their trades. Managers who obtain incentives from stock-based compensation would likely lose profit opportunities from legal insider trading, due to the greater visibility of their transactions. Blockchains would also deny managers opportunities to backdate compensation awards or covertly pledge shares for derivative transactions. Shareholder voting would become much more reliable and less costly. Companies might also use blockchains for real-time accounting, reducing the role of auditing firms, and for the execution of smart contracts, which would reduce the expected costs of financial distress and reduce the need for litigation. Together these changes could profoundly alter the relative power of managers, shareholders, lenders, regulators, and third party experts who interact in the corporate governance arena.

References

Admati, A. and Pfleiderer, P. (2009) The "Wall Street walk" and shareholder activism: exit as a form of voice, *Review of Financial Studies* **22**, 2445–2485.

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timon, J., and Wuille, P. (2014) Enabling blockchain innovations with pegged sidechains. Unpublished working paper, Blockstream.com.

Baiman, S. and Verrecchia, R. (1996) The relation among capital markets, financial disclosure, production efficiency, and insider trading, *Journal of Accounting Research* **34**, 1–22.

Bebchuk, L. and Jackson, R. (2012) The law and economics of blockholder disclosure, *Harvard Business Law Review* **2**, 39–60.

Bettis, C., Bizjak, J., and Kalpathy, S. (2015) Why do insiders hedge their ownership? An empirical investigation, *Financial Management* **44**, 655–683.

Bheemaiah, K. (2015) Why business schools need to teach about the blockchain. Unpublished manuscript, Grenoble École de Management.

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

Boucher, P. (2016) What if blockchain technology revolutionized voting? Unpublished manuscript, European Parliament.

Brav, A. and Matthews, D. (2011) Empty voting and the efficiency of corporate governance, *Journal of Financial Economics* **99**, 289–307.

Brochet, F. (2010) Information content of insider trades before and after the Sarbanes–Oxley act, *Accounting Review* **85**, 419–446.

Bushman, R., Piotroski, J., and Smith, A. (2005) Insider trading restrictions and analysts' incentives to follow firms, *Journal of Finance* **60**, 35–66.

Christoffersen, S., Geczy, C., Musto, D., and Reed, A. (2007) Vote trading and information aggregation, *Journal of Finance* **62**, 2897–2927.

Cicero, D. (2009) The manipulation of executive stock option exercise strategies: information timing and backdating, *Journal of Finance* **64**, 2627–2663.

Cohen, D., Dey, A., and Lys, T. (2008) Real and accrual-based earnings management in the pre- and post- Sarbanes–Oxley periods, *The Accounting Review* **83**, 757–788.

Collin-Dufresne, P. and Fos, V. (2015) Do prices reveal the presence of informed trading?, *Journal of Finance* **70**, 1555–1582.

Collin-Dufresne, P. and Fos, V. (2016) Insider trading, stochastic liquidity and equilibrium prices, *Econometrica* **84**, 1441–1475.

Cunningham, L. (2006) Too big to fail: moral hazard in auditing and the need to restructure the industry before it unravels, *Columbia Law Review* **106**, 1698–1748.

Edmans, A. (2009) Blockholder trading, market efficiency, and managerial myopia, *Journal of Finance* **64**, 2481–2513.

Edmans, A. (2014) Blockholders and corporate governance, *Annual Review of Financial Economics* **6**, 23–50.

Edmans, A., Fang, V., and Zur, E. (2013) The effect of liquidity on governance, *Review of Financial Studies* **26**, 1443–1482.

Edmans, A., Levit, D., and Reilly, D. (2016) Governing multiple firms. Unpublished manuscript, London Business School and University of Pennsylvania.

Ernstberger, J., Link, B., Stich, M., and Vogler, O. (2016) The real effects of mandatory quarterly reporting. Unpublished manuscript, Technische Universität München, Neue Masche, Friedrich-Alexander Universitaet Erlangen-Nuernberg and Ruhr Universität Bochum.

Fishman, M. and Hagerty, K. (1992) Insider trading and the efficiency of stock prices, *RAND Journal of Economics* **23**, 106–122.

Graham, J., Harvey, C., and Rajgopal, S. (2006) Value destruction and financial reporting decisions, *Financial Analysts Journal* **62**, 27–39.
Grossman, S. and Hart, O. (1980) Takeover bids, the free rider problem, and the theory of the corporation, *Bell Journal of Economics* **11**, 42–64.
Haber, S. and Stornetta, S. (1991) How to time stamp a digital document, *Lecture Notes in Computer Science* **537**, 437–455 (Advances in Cryptology—CRYPT0' 90).
Heron, R. and Lie, E. (2007) Does backdating explain the stock price pattern around executive stock option grants?, *Journal of Financial Economics* **83**, 271–295.
Holden, C., Jacobsen, S., and Subrahmanyam, A. (2013) The empirical analysis of liquidity, *Foundations and Trends in Finance* **8**, 265–365.
Hong, H., Lim, T., and Stein, J. (2000) Bad news travels slowly: size, analyst coverage, and the profitability of momentum strategies, *Journal of Finance* **55**, 265–295.
Hu, H. and Black, B. (2006) The new vote buying: empty voting and hidden (morphable) ownership, *Southern California Law Review* **79**, 811–908.
Kahan, M. and Rock, E. (2008) The hanging chads of corporate voting, *Georgetown Law Journal* **96**, 1227–1281.
Kahn, C. and Winton, A. (1998) Ownership structure, speculation, and shareholder intervention, *Journal of Finance* **53**, 99–129.
Kocherlakota, N. (1998) Money is memory, *Journal of Economic Theory* **81**, 232–251.
Kraft, A., Vashishtha, R., and Venkatachalam, M. (2016) Frequent financial reporting and managerial myopia. Unpublished manuscript, City University London and Duke University.
Kyle, A. and Vila, J. (1991) Noise trading and takeovers, *RAND Journal of Economics* **22**, 54–71.
Lazanis, R. (2015) How technology behind bitcoin could transform accounting as we know it, *TechVibes*, January 22.
Lee, L. (2016) New kids on the blockchain: how bitcoin's technology could reinvent the stock market, *Hastings Business Law Journal* **12**, 81–132.
Leland, H. (1992) Insider trading: should it be prohibited?, *Journal of Political Economy* **100**, 859–887.
Listokin, Y. (2008) Management always wins the close ones, *American Law and Economics Review* **10**, 159–184.
Malinova, K. and Park, A. (2016) Market design for trading with blockchain technology. Unpublished manuscript, University of Toronto.
Manne, H. (1966) *Insider Trading and the Stock Market*, Free Press, New York.
Maug, E. (1998) Large shareholders as monitors: is there a trade-off between liquidity and control?, *Journal of Finance* **53**, 65–98.
Metz, C. (2015) The bitcoin schism shows the genius of open source. *Wired*, August 19.
Nakamoto, S. (2008) Bitcoin: a peer-to-peer electronic cash system. Unpublished manuscript.
Nallareddy, S., Pozen, R., and Rajgopal, S. (2016) Consequences of mandatory quarterly reporting: the UK experience. Unpublished manuscript, Columbia University, Duke University, and Massachusetts Institute of Technology.
Norli, Ø., Ostergaard, C., and Schindele, I. (2015) Liquidity and shareholder activism, *Review of Financial Studies* **28**, 486–520.
Ronen, J. (2010) Corporate audits and how to fix them, *Journal of Economic Perspectives* **24**, 189–210.
Rosenbloom, P., Schlingemann, F., and Vasconcelos, M. (2014) Does stock liquidity affect incentives to monitor? Evidence from corporate takeovers, *Review of Financial Studies* **27**, 2392–2433.
Roulstone, D. (2003) The relation between insider trading restrictions and executive compensation, *Journal of Accounting Research* **41**, 525–551.
Schroeder, J. (2015) Bitcoin and the uniform commercial code. Unpublished manuscript, Yeshiva University.
Sisli Ciamarra, E. (2012) Monitoring by affiliated bankers on board of directors: evidence from corporate financing outcomes, *Financial Management* **41**, 665–702.

Swanson, T. (2015) Watermarked tokens and pseudonymity on public blockchains. Unpublished manuscript, R3CEV.

Szabo, N. (1994) Smart contracts. Unpublished manuscript.

The Economist (2015) The great chain of being sure about things. October 29.

Wright, A. and DeFilippi, P. (2015) Decentralized blockchain technology and the rise of lex cryptographia. Unpublished manuscript, Yeshiva University and Université Paris II.

Yermack, D. (2009) Deductio *Ad Absurdum*: CEOs donating their own stock to their own family foundations, *Journal of Financial Economics* **94**, 107–123.