NBER WORKING PAPER SERIES

CORPORATE GOVERNANCE AND BLOCKCHAINS

David Yermack

Working Paper 21802
http://www.nber.org/papers/w21802

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
December 2015

Corporate Governance and Blockchains
David Yermack
NBER Working Paper No. 21802
December 2015
JEL No. G20,G3

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. During 2015 many major players in the financial industry 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.

David Yermack
Stern School of Business
New York University
44 West Fourth Street, Suite 9-160
New York, NY 10012
and NBER
dyermack@stern.nyu.edu

Corporate Governance and Blockchains

I. Introduction

This essay explores the corporate governance implications of blockchain database technology. Blockchains have captured the attention of the financial world in 2015, and 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 use of blockchains to register equity issued by corporations. Blockchains can also hold debt securities and financial derivatives, which can be executed autonomously as "smart contracts."

These innovations have the potential to change corporate governance as much as any event since the 1933 and 1934 securities acts in the United States.

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). Simple 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's managers) and overcome corruption on the part of regulators, exchanges,

and listed companies. If a firm elected to keep its financial records on a blockchain, opportunities for earnings management and other accounting gimmicks could drop dramatically, and related party transactions would be 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 far less secrecy than under the current system. Managerial ownership could become much more transparent, with insider buying and selling detected by the market in real time, and chicanery such as the backdating of stock compensation becoming much more difficult, if not impossible. 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.

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 introduced by Nakamoto (2008) to track ownership of the virtual currency bitcoin. After more than six 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 to 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, and works of art.

Emerging markets may be among the first to see blockchain technology integrated into their stock exchanges and capital markets. 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 mPesa in Nigeria, and the high-profile efforts in 2015 by the government of Honduras to move its land registry onto a blockchain, provide vivid illustrations of the willingness to emerging economies to bypass older technologies and become early users of innovations that integrate economic data with information technology.

To date the most high-profile use of blockchain technology in corporate finance has occurred in the U.S. NASDAQ stock market, which launched a pilot project in May 2015 to evaluate the suitability of blockchains for registering and transferring shares. The Sydney and Frankfurt stock exchanges have also announced research programs to evaluate blockchain technology for their listed companies.[1] Lee (2015) 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.

[1] See Bradley Hope and Michael J. Casey, "A Bitcoin Technology Gets Nasdaq Test," *The Wall Street Journal*, May 10, 2015; Anna Irrera, "CME and Deustche Börse Join Blockchain Gang," *Financial News*, July 20, 2015; and Shaun Dummond, "ASX Considers Blockchain for Clearing and Settlement," *The Sydney Morning Herald*, October 26, 2015.

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 some of the critical constraints or assumptions (such as the rate as which new coins or shares might be issued). As implemented for bitcoin and other digital currencies, blockchains operate on a decentralized basis, with all participants in a network (such as all owners of bitcoins) sharing responsibility for updating them in real time. Proposed changes to the Bitcoin blockchain code occur only if they receive "consensus" from the network members via a passive process of adoption or rejection by more than 50%. The passive method of changing a blockchain's code by consensus might leave it vulnerable to various methods of sabotage and attack, either through brute force strategies resembling denial of service attacks, or more subtle divide-and-conquer strategies based on subterfuge or the exploitation of collective action problems. Overcoming these vulnerabilities appears to be an important, unfinished priority for promoters of blockchain technology. An alternative to the open Bitcoin blockchain is a closed, or "permissioned" blockchain open only to authorized users. While a permissioned blockchain might appear attractive for security reasons, it would lack some of the appealing features of an open blockchain, which does not rely on a controlling middleman to authorize and police transactions.

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

II How Blockchains Work

Tasca (2015) describes a blockchain as a "decentralized peer-validated time-stamped ledger." A blockchain consists of bundles of transactions, or "blocks," with each transaction indicating the asset to be transferred, the time of the transfer, the identity of the prior owner, and the identity of the new owner. The Bitcoin blockchain bundles together all network transactions approximately every 10 minutes and encrypts them into a new block through hashing. Blocks are "chained" together, because the header of each block contains a code the summarizes the contents of the previous block, and so forth, all the way back to the first block in the chain. This method allows network members to trace each unit of an asset (such as one bitcoin or one share of stock) through the sequence of all previous owners, back to the earliest point at which it entered the network. The sequential chaining of blocks makes fraud or forgery prohibitively difficult, since altering a prior entry would require altering all subsequent blocks. Bheemaiah (2015) provides an easily accessible discussion of these and other salient technical details, and The Economist (2015) offers a very useful general introduction and characterizes the blockchain as a "trust machine," since its algorithms report economic transactions with irrefutable precision without any need for verification by a 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.

Updating the blockchain is a computationally intensive task, and it could potentially be compromised by thieves, scammers, or spammers. The Bitcoin network ingeniously solves these problems by assigning the seignorage value of new bitcoins as the reward in an ongoing competition among certain network members operating "nodes." Nodes create new blocks every ten minutes by gathering transactions and combining them with a lengthy, unknown random

number that must satisfy certain criteria. Nodes compete by trial-and-error to find the correct random number, and the first successful one receives a reward of 25 new bitcoins, once the other nodes agree by consensus that the new block satisfies the correct criteria. The computation effort to find the random number provides a "proof of work" that raises the cost to saboteurs who might attempt to subvert the process. This competition among nodes is known as "mining," since the work required and reward received resembles the activity of mining for gold under a more ancient monetary system.

Up to now, the reward of new bitcoins has sufficed to attract enough miners to keep its blockchain current and reliable. However, 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 bitcoin network automatically adjusts the difficulty of the mining problem, raising or lowering the costs for miners to entice more into the network when needed. However, further growth of the network appears to require increasing the block sizes and/or shortening the update frequency, and proposed changes to accommodate such reforms have become hotly controversial at the time of this essay, as discussed below.

A blockchain's records are visible to all users of the network and also to outsiders who can view them via the Internet. It is often referred to as a "shared" or "distributed" ledger, since everyone participating in the network has a copy and shares responsibility for keeping it current. This wide distribution represents probably the blockchain's main difference from classical record-keeping, which is typically done on a central ledger under the control of a single bank, corporation, or government authority. Many problems can arise when one party controls access to a centralized ledger and has the ability to alter it. These potential problems range from

charging monopoly fees to corruption to technical failure, among others. The distrust of banks as custodians of monetary ledgers was the motivating factor that spurred Nakamoto (2008) to create the blockchain for Bitcoin.

If public access or visibility is a concern, a blockchain can restrict access only to its subscribers or authorized users through a gatekeeping mechanism often referred to as "permissioning." While this structure will keep saboteurs and other unwanted parties out of the network, it comes at a significant cost, since the ledger will be much less transparent, and governance will no longer take place by consensus. Instead, the gatekeeper who controls the permissioning process would become all-powerful and would need to be trusted by other network participants, re-creating exactly the problem that Nakamoto was trying to solve by distributing the Bitcoin blockchain to everyone.

Alternatives to distributed and permissioned ledgers are quickly emerging, all making use of blockchain technology. A "sidechain" offers a middle-ground solution, in which a company operates a private, permissioned ledger but periodically connects some aggregation of its transactions to a public, distributed ledger. Other platforms such as Etherium incorporate many features of blockchains while adding additional flexibility and functionality for users.

The Bitcoin blockchain has proven to be stable through six years of continuous use, and its reliability has led many developers of blockchain products to free-ride upon the bitcoin network. 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 memo field could be a "token" such as the share of stock. Miners will then bundle up the transaction into the next block, and the record of the bitcoin transfer will also provide proof of transfer of the stock. While this strategy seems appealing because it saves

development cost and takes advantage of Bitcoin's proven 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).

III Corporate Governance of Firms Listed on Blockchains

Registering corporate equity and debt securities on a blockchain would create numerous externalities related to faster, cheaper trade execution and greater transparency of ownership. 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 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.

A. Transparency of Ownership

Blockchains are distributed ledgers, meaning that a copy of the ledger is distributed and visible to all members of a network. In the case of a company with shares listed on a blockchain, all shareholders would be able to view the arrangement of ownership at any point in time, and to identify changes instantly as they occur. This transparency would have significant impacts upon the profit opportunities available to managers, institutional investors, and shareholder activists, among other groups. The incentives to acquire ownership and to liquidate it could change markedly if these transactions were observable in real time.

Of course, this claim assumes not only that a distributed ledger of share ownership can be

viewed by the public, but also that observers can identify the holders of individual shares and the counterparties of important transactions. For instance, if a manager sells shares of his own stock, I assume that the public will see not only 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 can be identified is a matter of debate. In principle, any computer archive can be inverted by a skilled cryptography expert, and law enforcement officials have successfully identified and prosecuted many illict users of the bitcoin network. Even without advanced forensics, one could rather easily match digital wallets with individual users by searching the raw data for a particular transaction pattern that is known to have occurred, such as an award of a certain quantity of restricted shares. However, a share owner can stay a step ahead by using a different digital wallet for each transaction or breaking transactions into small pieces using several wallets at once.

One would expect the identification of ownership on the blockchain to attract specialist research firms, who might earn fees by ascertaining the digital wallet addresses of individual managers or shareholder activists. Alternatively, regulators might require corporate insiders to disclose their digital wallet identifications under penalty of law.

1. Activists and Raiders

Building share positions secretly is a time-honored strategy of shareholder activists,

corporate acquirers, and institutional investors, all of whom wish to minimize their costs of acquisition by avoiding publicity as they buy. Every country has somewhat different disclosure requirements and thresholds that trigger these obligations. In the U.S., a patchwork of different regulations 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. The Securities and Exchange Commission is currently considering a reduction in the ten day period permitted for a 5% shareholder to file a public notice of his ownership position. As Bebchuk and Jackson (2012) write, this could deter activism by requiring earlier disclosure.

Registering shares on a blockchain would effectively negate any grace period for an activist trying to accumulate a block of shares, because acquisitions of shares could be observed instantly. 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 ownership registration.

2. Managers

Corporate managers obtain most of their incentives from stock compensation, either from stock options or restricted shares. 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 may transact on the basis of private information about the firm. One of the most significant aspects of the 2002 Sarbanes-Oxley Act was a reduction in the required filing period for managers following their acquisitions and dispositions

of shares. The previous rule, which required filing by the tenth day of the subsequent calendar month, was reduced to a regulation of disclosure within two business days. As shown by Brochet (2010), the market reacted more significantly to managers' transactions once these more timely reporting requirements took effect.

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 inside information and reap some of the profit associated with the valuable information they create. See Roulstone (2003).

Blockchain registration of a company's shares would undercut the effectiveness of equity-based managerment incentives. If managers' trades became observable in real-time, they would be less profitable. Real-time disclosure would also 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. A related problem for managers would be greater market awareness of when their shares are pledged as collateral for loans or in connection with derivative hedging products (Bettis, Bizjak, and Kalpathy, 2014). These strategies are used by managers to achieve a de facto liquidation of their equity incentives without incurring tax or signaling costs. In a blockchain registration system, the pledge of the share 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.

Finally, a blockchain registration system would 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). Blockchain entries are time-stamped and cannot be backdated, so they would pre-empt all types of share transfer backdating, a change that shareholder activists might view as value-improving even while managers might see it as costly.

B. Speed and cost of Trading

Stock trades in the U.S. generally require three business days for settlement to occur and ownership to move formally from seller to buyer. During this time 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 Corporation. Many people are involved in this process, necessitating the payment of fees directly (through commissions) and indirectly (through the bid-ask spread). In contrast, a sale of stock on the blockchain would be settled instantly and would not require any of these middlemen. While stock markets would probably continue to operate in some form to facilitate the meeting of buyers and sellers, liquidity would increase greatly due to the lower cost and faster speed of executing trades. Liquidity is a critical issue for portfolio managers and other investors both large and small. Improving liquidity would 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.

In corporate governance, greater liquidity should induce activist investors to play a

greater role, since the cost for them to acquire blocks of stock would be lower and exiting an investment should be easier. 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) shows that activists accumulate more shares when liquidity is greater. Note that this prediction differs from the hypothesis above, that greater transparency of trading would deter activists from investing. Therefore, the net effect of blockchain registration on the incentives for shareholder activism remains unclear.

C. Voting in Corporate Elections

Blockchain technology has been proposed as a platform for voting in all types of elections,[2] 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. 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 DeFillipi (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. 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

[2] See www.v-initiative.org for a well-known example.

currently do not use confidential voting.

1. Accuracy of Elections

The imprecision of vote tabulation 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?'"[3] While the vagaries of vote tabulation seem to introduce noise, Listokin (2008) presents results showing that close elections end up being decided in favor of management in a disproportionate number of cases. By implication, managements exploit their control of the voting process from start to finish to nudge close elections in their favor.

Blockchain voting would help resolve ambiguities about the outcomes of corporate elections and could greatly reduce management's ability to manipulate outcomes. The net effect would be more frequent election of dissident outside candidates representing shareholder activists or other groups and more frequent defeats of management proposals related to compensation and governance.

2. Defeating 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 a share. Hu and Black (2006) and Christoffersen, Geczy, Musto and Reed (2007) describe empty voting in detail. Many of these strategies rely on secrecy and can

[3]Kahan and Rock (2008), p. 1279.

culminate in investors appearing on election day with far more votes than expected. Some are not strictly legal but have succeeded due to the difficulties of observability 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 cast votes on the "wrong" side of a ballot question in order to create adverse outcomes that benefit the empty voter's other interests. 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. 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 enjoin voting of the shares.

D. Real-time accounting

Lazanis (2015) suggests that a firm could voluntarily post all of its ordinary business transactions on a blockchain. This would occur automatically if the firm used digital currency as its medium of exchange, but it could also be done by means of tokenization, as discussed earlier. Like all blockchain transactions, the firm's routine accounting data would be recorded

permanently with a time stamp, and it could not be altered ex-post. The company's entire ledger would then be visible immediately to any shareholder, lender, 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. While 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 be able to trust the integrity of the company's data, and costly auditors would not need to be hired to vouch for the accuracy of the company's books and records.

1. 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. The potential U.S. savings equals the total revenue of the accounting industry, which exceeds $50 billion per year. This sum represents the social cost for third-praty 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, 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 make their own decisions about depreciation schedules, marking assets to fair market value, and other 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 leading companies, market demand for their services

would probably continue in some form.

2. Earnings management

Real-time accounting on the blockchain would greatly reduce the opportunities for firms to engage in accounting gimmicks 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 over long 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 manipulated less 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.

3. Related party transactions

Real-time accounting on the blockchain would allow observers instantly to spot suspicious asset transfers and other transactions that have conflicts of interest. The disclosure rules of the U.S. and many other countries place a burden upon management to 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 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 distressed firms.

E. 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 could see their business shrink dramatically in a world in which many contracts became self-enforcing). A number of new platforms such as Etherium are designed to apply blockchain technology to execute smart contracts based upon simple events such as the passage of time or complicated contingencies such as future financial outcomes.

While 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 title to 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 the agency costs of debt. The willingness of a firm to enter into a smart contract could represent a pre-commitment 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 increasing the power of debtholders against equityholders. This would have beneficial effects such as reduced adverse selection in credit markets and a lower cost of debt. Boards of directors might

reconsider the need for banker-directors, who have classically filled a bonding role by signalling 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.

IV 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 the blockchain itself. A blockchain is operated by computer software. 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.

Just as is the case with a stock exchange, 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 be 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 among the participants in the event of disagreements.[4] In a closed, permissioned blockchain, negotiating these rules, including withdrawal rights, should be similar to the negotiation of a partnership agreement. In an open blockchain that can be joined by anyone,

[4] An excellent example would be the U.S. blockchain firm R3, which has organized a consortium of 25 leading banks to develop a way to trade assets among themselves using a distributed ledger system. It seems highly unlikely that all 25 banks 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.

governance can become much more complicated.

What could go wrong to provoke a governance crisis among the users of a blockchain? The most basic problem would be a so-called 51% attack, in which one participant on the blockchain controlled enough nodes 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. 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 for uploading the new, flawed 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.[5]

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 nodes on the network have discarded the old code and begun running the new one. The procedure is purely passive, 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.

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

Proposed changes to the code can simply be met with indifference and be ignored, while others my emerge as the byproduct of high-profile discussions 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 change the sizes of blocks in the Bitcoin blockchain.

V 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 and trade their shares, and stockholders may benefit from lower cost 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 would 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 lost 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 pledge shares for derivative transactions. Shareholder voting would become much more reliable and less costly. Companies may also use blockchains for real-time accounting, threatening the positions of auditing firms, and for the execution of smart contracts, which would reduce the costs of financial distress and reduce the need for litigation. Together these changes

could profoundly alter the relative power of managers, shareholders, regulators, and third party experts who coexist in the corporate governance space.

References

Bebchuk, Lucian A., and Robert J. Jackson Jr., 2012, "The Law and Economics of Blockholder Disclosure," Harvard Business Law Review 2, 39-60.

Bettis, Carr, John Bizjak, and Swaminathan Kalpathy, 2014, "Why Do Insiders Hedge Their Ownership? An Empirical Investigation," Financial Management 44:3, 655-683.

Bheemaiah, Kariappa, 2015, "Why Business Schools Need to Teach About the Blockchain," unpublished manuscript, Grenoble École de Management.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore, 2015, "Bitcoin: Economics, Technology, and Governance," Journal of Economic Perspectives 29, 213-238.

Brochet, François, 2010, "Information Content of Insider Trades Before and After the Sarbanes-Oxley Act," Accounting Review 85, 419-446.

Christoffersen, Susan E.K., Christopher C. Geczy, David K. Musto, and Adam V. Reed, 2007, Journal of Finance 62, 2897-2927.

Cicero, David C., 2009, "The Manipulation of Executive Stock Option Exercise Strategies: Information Timing and Backdating," Journal of Finance 64, 2627-2663.

Edmans, Alex, Vivian W. Fang and Emanuel Zur, 2013, "The Effect of Liquidity on Governance," Review of Financial Studies 26, 1443-1482.

Heron, Randall A., and Erik Lie, "Does Backdating Explain the Stock Price Pattern Around Executive Stock Option Grants?" Journal of Financial Economics 83, 271-295.

Hu, Henry T.C., and Bernard Black, 2006, "The New Vote Buying: Empty Voting and Hidden (Morphable) Ownership, Southern California Law Review 79, 811-908.

Kahan, Marcel, and Edward B. Rock, 2008, "The Hanging Chads of Corporate Voting," Georgetown Law Journal 96, 1227-1281.

Lazanis, Ryan, 2015, "How Technology Behind Bitcoin Could Transform Accounting as We Know it," TechVibes, available at http://www.techvibes.com/blog/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it-2015-01-22.

Lee, Larissa, 2015, "New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market," unpublished manuscript, University of Utah.

Listokin, Yair, 2008, "Management Always Wins the Close Ones," American Law and Economics Review 10, 159-184.

Metz, Cade, 2015, “The Bitcoin Schism Shows the Genius of Open Source,” Wired, August 19, available at http://www.wired.com/2015/08/bitcoin-schism-shows-genius-open-source/.

Nakamoto, Satoshi, 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System,” unpublished manuscript.

Norli, Øyvind, Charlotte Ostergaard, and Ibolya Schindele, 2015, “Liquidity and Shareholder Activism,” Review of Financial Studies 28, 486-520.

Roulstone, Darren, 2003, “The Relation Between Insider Trading Restrictions and Executive Compensation,” Journal of Accounting Research 41, 525-551.

Schroeder, Jeanne L., 2015, “Bitcoin and the Uniform Commercial Code,” unpublished manuscript, Cardozo School of Law.

Sisli Ciamarra, Elif, 2012, “Monitoring by Affiliated Bankers on Board of Directors: Evidence from Corporate Financing Outcomes,” Financial Management 41, 665-702.

Swanson, Tim, 2015, “Watermarked Tokens and Pseudonymity on Public Blockchains,” unpublished manuscript.

Szabo, Nick, 1994, “Smart Contracts,” unpublished manuscript, available at http://szabo.best.vwh.net/smart.contracts.html.

Tasca, Paolo, 2015, “Digital Currencies: Principles, Trends, Opportunities, and Risks,” Deutche Bundesbank research report.

The Economist, 2015, “The Great Chain of Being Sure About Things,” October 29.

Wright, Aaron, and Primavera DeFilippi, 2015, “Decentralized Blockchain Technology and the Rise of *Lex Cryptographia*,” unpublished manuscript.

Yermack, David, 2009, “Deductio *Ad Absurdum*: CEOs Donating Their Own Stock to Their Own Family Foundations,” Journal of Financial Economics 94, 107-123.