David Yermack
Professor
NYU Stern School of Business and
National Bureau of Economic Research

Smart contracts and corporate governance

1 Introduction

Smart contracts are commercial agreements implemented by the use of machinery and computer technology. As first described by Szabo's (1997) treatise, "The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive." The author points out the smart contracts are hardly new, with the mechanical candy vending machine, introduced in 1880s Britain, representing perhaps the earliest example.

Advances in information technology have made smart contracts more and more common in routine commerce. Today, the advent of blockchain technology and its implementation on flexible contracting platforms such as Ethereum have greatly expanded their potential use.

Smart contracts automate the performance by one or both sides to an agreement, and typically they cannot be rescinded or interrupted without the consent of both parties. Szabo (1997) offers the example of a consumer automobile loan in which the car serves as collateral and the borrower agrees to a fixed number of monthly payments. If the borrower misses a payment, a computer would remotely and automatically shut off the borrower's access to the car's ignition system; a more up-to-date example would probably have the car drive itself autonomously back to the lot of the lender.

The certainty of performance of a smart contract offers clear potential benefits. In the case of the vending machine, negotiation costs between buyer and seller are driven to zero, and the buyer has no need to worry about strategic default or other forms of moral hazard by the seller. In the car loan example, verification and enforcement costs disappear, since the lender does not need to hire a lawyer to go to court and obtain a lien to repossess the collateral from the borrower, and then hire a repo man to retrieve the vehicle. In this case, the seller does not need to worry about strategic behavior on the part of the buyer.

This screening out of moral hazard behavior will have the effect of removing from the market those parties who may intend to default on their obligations, improving the credit quality of the overall pool and driving down the cost of capital. In short, by guaranteeing performance, smart contracts reduce the need for trust in commercial relationships. Trustless contracting has become a common theme motivating the creation of digital currency and other blockchain applications.

At the same time, smart contracts certainly create new risks and problems. In the example of the car loan, one would not want the ignition to autonomously deactivate if the borrower is operating the vehicle on a crowded highway at rush hour, for instance. One might also not want to rule out strategic non-performance in all states of the world, as shown by Posner's (1973) famous popularization of

the idea of "efficient breach" of contracts, a foundational concept in the Law and Economics literature.

2 Smart contracts in corporate governance

Jensen and Meckling's seminal (1976) article on agency costs describes the firm as a "nexus of contracts" between suppliers of capital, skilled and unskilled labor, raw materials, customers, and other groups. The growing interest in smart contracts naturally leads to the question of how corporate governance might change if more and more of these relationships become automated. Some applications, such as self-executing derivative securities, are easy to anticipate, while others, such as self-enforcing labor agreements or employment contracts, may be far off but could also offer opportunities for joint gains between contracting parties. Like any new or emerging technology, smart contracts surely pose risks that may not yet be understood.

3 Three examples

In this section, I discuss three simple applications of smart contracts in corporate governance, in the areas of derivative securities, secured debt, and equity share registration. These examples are meant to be introductory and only hint at the possibility for more elaborate smart contracts.

3.1 Financial derivatives

Many aspects of a firm's capital structure involve contingent claims that can be exercised or extinguished under certain future conditions. In some cases, these involve a choice by the security holder; representative examples would include executive stock options or convertible debt, either or which may be converted to shares at a certain fixed price during a limited future exercise period. Other derivatives are intended to execute automatically if certain conditions are satisfied; these include instruments such as credit default swaps, which pay off to outside investors if a company defaults on its debt, and Contingent Convertible ("CoCo") debt securities, which might be issued by a bank and convert into equity if the bank's equity falls below the regulatory minimum requirement.

In all these examples, the exercise decisions could easily be automated by smart contracts. If a choice by the security holder is required to trigger the exercise, the smart contract could be programmed to execute when certain optimality conditions are achieved in the marketplace. This would overcome well-known problems in which investors sometimes exercise options or convert debt at sub-optimal times. If conversion of a security is contingent on a future event, again a smart contract could be used to verify the contingency continuously and automatically execute the conversion if the contingency is ever met. This would save costs of verification and potential litigation, while also avoiding strategic behavior sometimes seen in the marketplace to forestall the triggering of contracts.

3.2 Corporate debt

Companies often pledge collateral and make various balance sheet commitments as conditions of obtaining loans. If a company cannot stay in compliance with these loan covenants, in theory a process should begin in which the lender can obtain title to the collateral and demand repayment of the remaining loan balance. In practice, companies have recourse to judicial bankruptcy procedures that often forestall the lender's recoveries and provide legal incentives for the borrower and lender to renegotiate.

A smart contract could short-circuit the bankruptcy process by automatically conveying collateral from borrower to lender if a covenant is violated. In principle, compliance could be monitored in real time, and not just on the four days of the year in which a firm publishes its balance sheet. The contract could also execute other financial transfers and governance changes immediately if a default event occurs.

While the description above is quite general, the reader should see immediately that smart contracts can potentially resolve financial distress much more quickly and cheaply than the judicial processes that operate in most countries. Contracting around the judicial resolution of financial distress has for years been a closely studied topic in the finance and governance literatures. With self-executing smart contracts, many costly negotiating strategies involving brinksmanship and risk-shifting might be precluded, generating net savings that could be shared ex ante by the borrower and lender.

3.3 Share registration

Over centuries, stock markets have evolved elaborate systems for the custody, lending, and voting of shares of stock. Many investors delegate these tasks to brokers, for reasons that include cost savings, tax avoidance, privacy, and simplicity. The involvement of these custodians as intermediaries between companies and their own shareholders has led to many problems in areas such as payment of dividends and accurately tabulating votes, as described by Kahan and Rock (2008).

A recent fiasco involving the 2013 management buyout of Dole Food Co. vividly illustrates the weaknesses of the current share registration system in the U.S.A. After years of litigation over the buyout price, a court in Delaware in

2017 increased the per-share buyout price from USD 13.50 to USD 16.24. Owners of more than 49 million shares made legal claims for the increased payment, but the company had less than 37 million shares outstanding. Causes of this large discrepancy still remain partly unexplained, but observers have blamed the difference on the decentralized custodial system, in which each brokerage essentially keeps track of its own investor accounts and often permits shares to be lent out to short sellers. A short seller then sells the shares to other investors, without the knowledge of the ultimate owner whose shares are held in custody. In the case of Dole, there appear to have been millions of shares sold short, and the short sellers rather than the company should be liable for the increased payment of USD 2.74 per share. However, the buyers of these shares had no idea they were buying from short sellers, and they would have applied for payment from the company. All of this should be sorted out by the intermediary brokerages, but with the passage of four years, the failures and mergers of various firms, and the unexpectedly generous court decision, it has proven impossible to locate all the responsible parties.

Smart contracts seem like a straightforward solution to the types of problems seen in the Dole example and at

other companies. If a share of stock existed virtually on a blockchain, it could be embedded with smart contracts that could, variously, transfer dividend payments from the account of a short-seller to the account of the buyer, sell securities when margin calls are triggered against leveraged investors, and prohibit the double-voting that frequently occurs if shares are lent out by a custodian without knowledge of the true owner.

4 What could go wrong?

Smart contracts have many potential risks. They could autonomously execute in situations that neither party anticipates nor would wish for, causing irreversible losses or collateral damage to third parties. They may invoke other smart contracts, in a sequence that causes a cascade of escalating losses or so-called "death spiral" of a firm. The ground rules for interrupting smart contracts or resolving disputes ex post are very unclear, and perhaps non-existent.

Purists sometimes take a "code is law" view of smart contracts, implying that the parties must follow the consequences of the contract's written code if disagreements or unforeseen circumstances lead to outcomes that either party regrets. This viewpoint leaves no room for intervention by courts, and it puts a great burden upon the two parties to inspect and fully understand the written code underlying a contract before they implement it. In practice, it may not be possible for the parties to exclude courts from intervening if and when smart contracts run amok, and they may potentially assign liability not only to one or both of the parties, but also to programmers, blockchain hosts, and other entities involved in creating or providing the platforms for smart contracts.

An object lesson exists in the experience of TheDAO, a "decentralized autonomous organization" on the Ethereum blockchain that became the target of a successful hack in 2016. A DAO is essentially an organization run by computer code, with no human managers or employees. TheDAO was an ambitious attempt to create a decentralized venture capitalist that would facilitate a voting process for investors to select from a menu of potential start-up investment proposals.

TheDAO astonished investors by attracting USD 150 million worth of investment (in ether tokens) in a 28-day crowdfunding period that began on April 30, 2016, despite warnings from observers and analysts that the underlying code left it vulnerable to hacking. As feared by these commentators, a theft did occur on June 18, with the attacker – who has still not been identified – draining about USD 60 million of ether from TheDAO into a cloned "child DAO." Siegel (2016) prevents a lucid account of these events.

In the aftermath of this catastrophe, adherents to the "code is law" philosophy felt that TheDAO's investors had learned a hard lesson about the need to inspect smart contracts carefully before entering into them. However, the sponsors of Ethereum, who technically had no role in TheDAO, decided otherwise, and proposed several possible interventions. These included amending the Ethereum blockchain's code to isolate the assets stolen by the hacker, so that they could not be moved or otherwise spent, or rewinding the blockchain itself to negate the transactions implemented by the hacker.

The latter approach, essentially "rewriting history" on the Ethereum blockchain, was ultimately supported by about 85% of the user community and was implemented. However, the 15% minority that disagreed continued to use the original Ethereum blockchain, renaming it "Ethereum Classic" and essentially creating a schism that caused two versions of the ether currency to begin circulating. The split has endured to this day; as of the date of this writing, the Ethereum currency has a market capitalization of about USD 21 billion, while Ethereum Classic's currency is worth about USD 1.5 billion, both much higher than the USD 1 billion value of the original Ethereum at the time of the hack in June 2016.

This so-called "hard fork" in the Ethereum blockchain may have satisifed many normative tests of fairness, and it may even have resembled the outcome that a court would have imposed if litigation had occurred. However, it created a troubling precedent, showing that the sponsors of a blockchain have the power to rewind it as a type of remedy if a smart contract runs off the rails. The conditions under which such interventions might occur in the future seem uncertain at best, and victims of smart contracts with unhappy endings will surely try to invoke them, citing the precedent of TheDAO.

Conclusion

Smart contracts, which use information technology for verification and execution, represent a promising facet of the Fintech movement. They may solve longstanding problems of cost and delay in contract enforcement, but their greater potential may be in screening from the credit markets potential borrowers who are predisposed to moral hazard problems such as strategic debt default. In the corporate governance area, smart contracts may reduce numerous agency costs that arise between investors, managers, and other parties. However, like any new technology smart contracts may be misunderstood and create new problems, and today's markets are still in the early stages of discovering the potentials and pitfalls of these instruments.

References

Atlas, R. D. 2001. Where Donald Trump Sees Trouble in Atlantic City. Bondholders See an Effort to Cut a Deal. The New York Times. October 31.

Birmingham, R. 1970. Breach of Contract, Damage Measures, and Economic Efficiency. In: Rutgers Law Review 24. 273–292.

Jensen, M. C. and W. H. Meckling. 1976. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. In: Journal of Financial Economics 3. 305–360.

Kahan, M. and E. Rock. 2008. The Hanging Chads of Corporate Voting. In: Georgetown Law Journal 96. 1227–1281.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/bitcoin.pdf.

Posner, R. 1973. Economic Analysis of Law. Little, Brown and Company. Boston.

Siegel, D. 2016. Understanding The DAO Attack. Coindesk. June 25.

Szabo, N. 1997. Formalizing and Securing Relationships on Public Networks, First Mind 2:9. Available at http://ojphi.org/ojs/index.php/fm/article/view/548/469.