2017

Can Blockchain Solve the Holdup Problem in Contracts?

Richard T. Holden
Richard.Holden@chicagounbound.edu

Anup Malani
dangelolawlib+anupmalani@gmail.com

CAN BLOCKCHAIN SOLVE THE HOLDUP PROBLEM IN CONTRACTS?

Richard Holden and Anup Malani[1]

Abstract

A basic problem in contracting is holdup: after one party has made relationship-specific investments, the other party refuses to perform unless the first one offers better terms than the original contract. Such renegotiation deters relationship-specific investments and reduces the value of trade via contract, which can either result in no trade or more trade within firms. A classic example is the case of *Alaska Packers Association v. Demenico*, 117 F. 99 (9th Cir. 1902). Economists have devised solutions – called renegotiation design and revelation mechanisms – to these problems, but they are presently difficult to implement as they require very strong commitment to specific trades, a feature that the current contract–writing wherewithal and court system cannot provide. However, blockchain, a new technology that creates a distributed, unalterable and open ledger, combined with so-called smart contracts, automated scripts that execute contracts, can provide such commitment. Blockchain can thereby either make original contracts unable to be renegotiated or enable the commitment required for renegotiation design or revelation mechanisms. In this manner, blockchain technology and smart contracts can increase the gains from contractual trade, reducing the size of firms and increasing economic output.

I. INTRODUCTION

It has long been understood that transactions costs reduce gains from trade, specifically arms-length trade between legally distinct parties in the marketplace. These costs reduce the amount of efficient trade, as noted by Professor Coase in *The Problem of Social Cost*,[2] and can increase the role and size of firms, as parties switch from using contracts to transact in markets, to organizing economic activity within firms. This was also famously noted by Coase, but in *The Nature of the Firm*.[3]

While the paradigmatic form of transactions costs that Coase's had in mind was haggling between parties, later scholars, such as Professor Williamson, highlighted another important and pernicious transaction cost: holdup.[4] If contracts are not perfectly complete,[5] and one party makes a relationship-

[1] UNSW and NBER; University of Chicago and NBER. We thank Ilya Beylin, Anthony Casey, Stacy Rosenbaum, and Massimo Young for comments.

[2] R. H. Coase, The Problem of Social Cost, 3 JOURNAL OF LAW AND ECONOMICS 1, 15-19 (1960).

[3] R.H. Coase, The nature of the firm, 4 ECONOMICA 386, 395 (1937).

[4] Oliver E. Williamson, MARKETS AND HIERARCHIES: ANALYSIS AND ANTITRUST IMPLICATIONS 9–10, 26–28 (Free Press 1975).

[5] By this we mean contracts do not specify the terms of trade for every possible state of the world. See Patrick Bolton and Mathias Dewatripont, CONTRACT THEORY, MIT Press, Cambridge MA, 2005, chapters 11-12.

Electronic copy available at: https://ssrn.com/abstract=3093879

specific investment, the counterparty can threaten not to perform in order to extract part of the difference between the value of the investment to the two parties and the value in its next best use.[6]

The classic example in contracts casebooks is *Alaska Packers Association v. Demenico* (1901).[7] Defendant Alaska Packers Association hired plaintiff fishermen in San Francisco to fish for salmon in Alaska and deliver the fish to Pyramid Harbor, Alaska, where the defendant operated a cannery. The original contract paid each fisherman $50 for the season plus two cents for each salmon caught. Once the defendant sailed plaintiffs to Alaska, they refused to fish unless their pay was increased to $100 for the season plus two cents for each salmon. Defendant agreed, but when the plaintiffs returned to San Francisco and sought payment under the revised contract, the defendant refused and paid the fishermen their originally agreed-upon wages.[8] The plaintiffs sued. The district court sided with the plaintiffs, on the theory that the defendant was not held up: it could have rejected the fishermen's demand.[9] The appellate court sided with the defendant and said there was no consideration for the revised agreement.[10]

Subsequent scholars and modern courts have interpreted the case to stand for the proposition that contract terms that are the result of renegotiation under duress, e.g., following investment, are invalid. In their view, the defendant had made a relationship-specific investment, chartering a ship to take the plaintiffs to Alaska, and, having delivered on their promise, were being held-up by the plaintiffs.[11]

Although that rule scholars and modern courts extract from *Alaska Packers* on its face seems to address the problem of holdup, it may not do so in practice. For the rule to work, courts must understand and interpret the facts of the case correctly. But they might not even have done this correctly in *Alaska Packers*. The district court and the appellate court ostensibly agreed on facts[12] but came to different results.[13] In addition, Professor Threedy has investigated the historical data and the factual record of the case, and found a number of factual errors that, if corrected, could have altered the decision in the case.[14] First, Alaska Packers may not have been in as much duress as the Appellate Court thought, as they had leverage against the fisherman[15] at the time of the renegotiation and they had insurance against renegotiation.[16] Second, some facts that suggest that the fishermen's costs were higher than

---

[6] This description of the holdup problem borrows from Richard Holden & Anup Malani, Renegotiation Design by Contract, 81 THE UNIVERSITY OF CHICAGO LAW REVIEW 151, 157-160 (2014).
[7] *Alaska Packers' Ass'n v. Domenico*, 117 F. 99 (9th Cir. 1902).
[8] *Domenico v. Alaska Packers' Ass'n*, 112 F. 555 (N.D.Cal. 1901)
[9] *Domenico*, 112 F. at 557.
[10] *Alaska Packers' Ass'n*, 117 F. at 105.
[11] See, e.g., Richard A. Posner, Gratuitous Promises in Economics and Law 46, in 56 THE ECONOMICS OF CONTRACT LAW (Anthony T. Kronman & Richard A. Posner, eds. 1979); Marvin A. Chirelstein, CONCEPTS AND CASE ANALYSIS IN THE LAW OF CONTRACTS 65 (3d ed. 1998); Mary Lou Serafine, Note, Repudiated Compromise after Breach, 100 YALE L.J. 2229 (1991).
[12] *Alaska Packers*, 117 F. at 101.
[13] Compare also, e.g., *Goebel v. Linn*, 11 N.W. 284 (Mich. 1882) and *Smithwick v. Whitley*, 67 S.E. 913 (N.C. 1910) with *Austin Instrument, Inc. v. Loral Corp*., 272 N.E.2d 533 (N.Y. 1971) and *Selmer Co. v. Blakeslee-Midwest Co*., 704 F.2d 924 (7th Cir. 1983).
[14] Debora L. Threedy, A Fish Story: Alaska Packers' Association v. Domenico, 2000 UTAH L. REV. 185 (2000).
[15] They could have denied the fisherman food while at Pyramid Harbor. Threedy, *supra* note 14, at 217.
[16] Alaska Packers Association were part of an association of canneries that insured each other against losses at any specific cannery, including the one at Pyramid Harbor. Moreover, not only was the cannery at Pyramid Harbor was

Electronic copy available at: https://ssrn.com/abstract=3093879

they expected.[17] Third, the fisherman seemed to have signed a low-price contract but only realized it when they arrived at Pyramid Harbor, where they found other fisherman making double their wage. Each of these facts point in different directions. But to us, they make clear that it is quite possible the defendant was actually held up but that a court could reasonably have come to the conclusion that they were not, as the District Court did. Even the possibility that renegotiation would be sanctioned by courts is enough to discourage investment and even trade.

The fact pattern in *Alaska Packers*' in not unique. Many transactions have a similar structure: A buyer B and a seller S want to trade some "widget". The buyer has valuation v and the seller has come cost c. The joint surplus is $v - c$, and the price is set to split that surplus. The buyer is able to make an investment that increases its valuation to $v' > v$ while the seller is able to make a separate investment to reduce its cost to $c' < c$. These investments may be worthwhile investments, i.e., they increase the joint surplus less than they cost. But after one or the other party invests, the other can withhold performance to obtain a better price.[18] Transactions with this basic structure are the subject of this paper.

We will elaborate on the holdup problem using a modern example that is easier to relate to: Apple buying the glass for its iPhone smartphone from the supplier Corning. Corning can invest to customize those components for Apple's unique phone design (as opposed to, say, Samsung's phone) and Apple can invest by designing and marketing features enabled by properties of Corning's glass. After either Apple or Corning invests, the other party can try to renegotiate their contract to its own advantage.

There are a number of ways in which parties can presently try to protect themselves from renegotiation. First, if all the facts were verifiable by courts, then the parties could simply write a contract that stipulated payoffs for each possible set of facts—a so-called "state contingent contract". This not only requires a great deal of information, but, as we pointed out in the *Alaska Packers'* example, this is not feasible as courts have imperfect fact-finding and -interpretive capacity.

Second, parties could use one of the several renegotiation mechanisms that contract theory economists have identified to solve the hold-up problem, such as default trades plus take it or leave it offers,[19] or

---

a small component Alaska Packer's total production, but that cannery had other suppliers of fish – local Native American tribes. Threedy, *supra* note 14, at 200, 212, 215-216.

[17] The fishermen were trained that nets were not to be reused season to season. Alaska Packers, however, had bought a new type of net that allowed reuse. It is possible the fishermen reasonably thought the nets were inadequate, though it is also possible a court could say that in fact the nets were adequate. Threedy, *supra* note 14, at 205-208.

[18] See Philippe Aghion, et al., Renegotiation Design with Unverifiable Information, 62 ECONOMETRICA 257, 259 (1994) (presenting an early formal description of the model in the text), Bengt Holmstrom, Moral Hazard in Teams, 13 THE BELL JOURNAL OF ECONOMICS 324, 326 (1982) (presenting a more general version of the problem), and Oliver Hart & John Moore, Incomplete Contracts and Renegotiation, 56 ECONOMETRICA 755, 757 (1988) presenting a simpler formal description of the problem wherein only one party makes a relationship specific investment). See also Williamson, *supra* note 4, at 9–10, 26–28, Victor P. Goldberg, Regulation and Administered Contracts, 7 BELL J. ECON. & MANAGEMENT SCI. 426, 439-41 (1976), and Benjamin Klein, et al., Vertical Integration, Appropriable Rents, and the Competitive Contracting Process, 21 THE JOURNAL OF LAW & ECONOMICS 302 (1978), for non-formal discussions of the holdup problem.

[19] Philippe Aghion, et al., Renegotiation Design with Unverifiable Information, 62 ECONOMETRICA 257, 263-625 (1994).

Electronic copy available at: https://ssrn.com/abstract=3093879

option contracts.[20] But each of these themselves require commitment otherwise they are vulnerable to renegotiation.

Third, the parties could use penalty clauses (liquidated damages greater than economic damages), such as a poison pill adapted to this setting, to ensure commitment in the renegotiation mechanism context or even in the original contract. Penalty clauses tend to be struck down by courts.[21] Moreover, a poison pill-type clause can be enjoined between the point of investment and the time the pill-type device is implemented. Finally, efforts to make the poison pill more robust end up looking a lot like the smart contracts on blockchain solution we present.[22]

Alternatively, courts could always enforce original contracts which contain provisions that bar renegotiation.[23] Even this would be inadequate as it is possible that, when one party holds up the other, they demand not just a different price, but also a degree of silence that makes it difficult to sue for the original contract terms.[24]

Our claim in this paper is that smart contracts on blockchain networks can reduce the risk of renegotiation and thereby hold-up.[25] Blockchain is a computer science innovation that enables the creation of a distributed, open and unalterable ledgers. What that means is that a transaction on a computer network with blockchain infrastructure, also called a blockchain network, is witnessed by others on the network (distributed), is made public to everyone on the network (open), and cannot be changed without a tremendous amount of computing power or cost (unalterable). Smart contracts are

---

[20] Georg Noldeke & Klaus M. Schmidt, Option Contracts and Renegotiation: A Solution to the Hold-up Problem, 26 THE RAND JOURNAL OF ECONOMICS 163, 168-71 (1995).

[21] Edward Allan Farnsworth, FARNSWORTH ON CONTRACTS 845 (Aspen Publishers. 2003).

[22] The pill-type device can take many formats. The strongest one we can think of is a machine that literally burns a holding-up party's cash money when it detects a deviation from the original terms of the contract. Smart contracts on blockchain allows one to mimic the cash-burning machine with digital fiat currency and blockchain allows the smart contract to see all other transactions the parties engage in. See infra Section V.A.

[23] Alternatively, courts could simply disallow renegotiation. However, some renegotiations are good: parties who experience changed circumstance that yield high joint surplus with a different exchange should be allowed to renegotiate. In other words, maybe parties should be able to bar renegotiation when they know there is no risk of changed circumstance, but courts should not.

[24] E.g., the party could require delayed payment so that it is too difficult for the held-up party to sue because of depreciated evidence or statute of limitations. Of course, the perpetrator of the holdup must offer the other party a higher price, as silence of the victim itself comes at a cost to the perpetrator. They could renegotiate in a separate contract and withhold payment under that separate contract until the statute of limitations on the original contract runs out, or evidence that would assist the victim in litigation deteriorates.

[25] In a contemporaneous working paper, Professors Casey and Niblett make the claim that, using big data and machine learning, code will be able to draft contracts (which they term self-driving contracts) knowing only the parties objectives. They argue such contracts will eliminate the problem of ex post holdup. Anthony Casey and Anthony Niblett, Self-Driving Contracts, working paper (Aug. 8, 2017). Our analysis differs from theirs in that it assumes that relationship-specific investments or states are non-verifiable to third parties, including the server running the code. Without that knowledge, the self-driving contract could not update the contract. The parties can, however, devise ways to make such information verifiable with renegotiation design or revelation mechanisms. To the extent that the self-driving contract is written with these mechanisms, the self-driving contract and the smart contracts in this paper are the same thing. However, even these require a high degree of knowledge as explained in Section II.D.1. If that information is not available, self-driving contract are not available. However, parties can still write a smart contract to enforce the original contract prior to renegotiation, as we explain in section V.

computer scripts that execute transactions, including transactions that constitute mutual promises between contracting parties, now and in the future. When created on blockchain, the future transactions envisioned in the smart contract are automatically executed and, because of the inalterability of the blockchain, cannot practically be stopped. Thus, smart contracts on blockchain are able to impose liquidated damages that cannot be renegotiated, or enjoined, or reversed by courts. This allows the parties either to commit to the original contract or to renegotiation mechanisms that both protect against holdup while allowing for mutually-preferred modifications due to changed circumstances.

Our proposed solution is not guaranteed to work, but we think it is a significant improvement over the status quo. The biggest obstacle to our solution is the government. It is possible courts or Congress would ban smart contracts and/or blockchain. But we believe blockchain has enough value, especially to the financial services sector, that collateral costs will deter the government from banning our solution. The government could ban specific uses of smart contracts and blockchain, e.g., stopping automation of future promises or certain contract penalty provisions. But this is unlikely as both parties to a contract want these terms ex ante. It is only ex post that one party does not prefer them. As with liquidated damages, we think the risk of court intervention is limited to cases of bargaining-power imbalance. Finally, our solution cannot overcome the so-called common knowledge problem that limits the power of renegotiation mechanisms to prevent holdup. To be sure, neither can existing contracting techniques. However, blockchain, by making all transactions open, may be able to reduce the severity of the common knowledge problem to some extent.

Our paper is a contribution not just to the literature on how to practically address the holdup problem,[26] but will also help courts understand what blockchain and smart contracts do. Towards those ends, Section II illustrates the hold-up problem, renegotiation mechanisms and the common knowledge barrier. Section III explores how pre-blockchain techniques have and could address the hold-up problem. Section IV summarizes blockchain and smart contracts. Section V shows how smart contracts on blockchain can help reduce holdup better than existing techniques. Section VI examines some of the limitations of smart contracts on blockchain. The conclusion makes predictions about the implications of our argument for the size of firms and output. It also speculates about the benefits of smart contracts and blockchain for contract law more generally.

II. THE HOLD-UP PROBLEM, RENEGOTIATION AND REVELATION MECHANISMS, AND THE COMMON KNOWLEDGE PROBLEM

In order to illustrate the holdup problem and its possible theoretical solutions, we use a recent example that should be familiar to readers, at least those familiar with smart phones. The buyer in our example is Apple, an original equipment manufacturer ("OEM") of the iPhone smartphone and the seller is Corning, an important component manufacturer which produces "Gorilla Glass". Our contention is not that Apple and Corning's contract actually had a hold-up problem, but that it might have and that we can therefore use it to illustrate some of the impacts of hold-up and solutions to hold-up.

[26] For an example of such work, see, e.g., Holden and Malani, *supra* note 6, at 155-156.

A. The hold-up problem and its impacts

Suppose Apple and Corning want to enter into a relationship wherein Corning provides 1 unit of a good ("Gorilla Glass" or "glass") at price p per unit.[27] The value generated by trade depends on Apple's valuation for the glass, v and Corning's cost of producing the glass c.

The timing of the relationship is as follows. First, the parties contract. Second, they make their investments non-cooperatively and simultaneously. Third, they both learn v and c. Finally, the contract is executed.

At the time of contracting, the precise values of v and c are not known since they depend on investments made by Apple and Corning. Suppose that v can be either \$40 or \$32 and correspondingly *c* can be \$16 or \$10.[28] Apple's investment affects the probability that *v* is high (or low) and Corning's investment affects the probability that *c* is high (or low). These investments are privately costly to Apple and Corning, costing each \$5. One can think of Apple's investment as marketing of the iPhone thus increasing sales volume or as Apple making other features of the iPhone more complementary with strong glass—say by having a smaller form-factor or reduced bezel or adding a face recognition system that eliminates the need for a thumbprint ID-enabled home button and allows the screen to take up the entire front of the smartphone. One can think of Corning's investment as improving the strength of glass, especially larger pieces of glass, or lowering the cost of production.

The parties do not write fully state-contingent contracts that specify p and the probability of trade q[29] for each combination of v and c and they only invest after they contract because, in reality, there are unanticipated innovations, opportunities or challenges that arise after contracting but before delivery. Real-world examples include Samsung's surprise introduction of a glass screen that folds around the edges of their Galaxy phone.[30] Corning felt pressure to match that. Another real-world example is Apple's surprise filing of a facial recognition system that increases the value of a larger glass plate front from Corning.[31] Apple would not want to announce the patent earlier for fear that competitors or even suppliers might file their related patents earlier.

---

[27] Instead of dealing quantities traded, our example will deal with the probability of trade. However, our example does not depend on the buyer only obtaining one unit of the good in question because we can define a unit a lot of any arbitrary number of submits, e.g., crates of 1000 individual glass plates. In this context, purchase of 500 glass plates can be described as a one-half probability of buying 1 crate of glass plates.

[28] The numbers in this example borrow heavily from a numerical example in Malani and Holden, *supra* note 6, at 164-169.

[29] See *supra* note 27.

[30] See Samsung Galaxy 6.

[31] See Jordan Crook, "This Apple patent application could describe facial recognition for the next iPhone," TECHCRUNCH (July 6, 2017), available at https://techcrunch.com/2017/07/06/this-apple-patent-could-describe-facial-recognition-for-the-next-iphone/ (last visited on Oct. 2, 2017).

With the numbers we have chosen in our example, the socially efficient thing to do is for both parties to make the investments, since both have a marginal value above their marginal cost ($8 compared to $5 for Apple's investment and $6 compared to $5 for Corning's). If the investments are made then total surplus is $40 − $10 − $5 − $5 = $20.

The essence of the hold-up problem, however, is that Apple and Corning will underinvest in the absence of the ability to contract on the investments (or values/costs) if they cannot prevent renegotiation. To see this, consider Corning, and suppose they make their privately costly investment. Once Apple's value for the glass and Corning's cost of producing it is realized, the parties will renegotiate the price, since contracting was incomplete at the start of the relationship. Assuming, for simplicity, that the parties evenly split the incremental surplus generated (as would arise as a result of the Nash bargaining solution) then the price will be adjusted so that Corning only gets half of the $6 that it increased total surplus by, that is $3. Anticipating this at the investment stage Corning compares the $3 benefit with the $5 cost and will not invest. Analogously, Apple will compare a $8/2=$4 benefit with a $5 cost and likewise will not invest. This means that, in the presence of hold up, neither party will invest, Apple's valuation will be low and Corning's cost high, and total surplus will be $32-$16=$16.

As our numerical example illustrates, hold-up reduces economic surplus. It is thus natural, therefore, that economists have spent considerable effort[32] exploring how its impact can be mitigated, in circumstances where it cannot be avoided due to limitations of the contracting environment.

B. Using renegotiation-design mechanisms to address hold-up

The difficulties with holdup derive from subsequent the renegotiation of prices. The logic behind the mechanisms economists have designed to tackle the hold-up problem stem from the observation that if this renegotiation could be structured differently then perhaps the social optimum could be obtained despite hold-up. Chung (1991) and Aghion, Dewatripont and Rey (1994) are leading examples of this approach. We illustrate how renegotiation design mechanisms work using the mechanism in Aghion, Dewatripont and Rey (1994), henceforth "ADR". In Appendix I, we illustrate another important renegotiation mechanism based on options contracts and attributable to Noldeke and Schmidt (1995).

The ADR mechanism has two components. The first component is a default trade that can always be requested by one party, even if it is held-up. This default option is structured to give that party (say the seller) a full return to its investment for sure. This needs to be enforceable with a specific performance remedy or a liquidated damages remedy that strongly incentivizes specific performance if the party with the default option requests the default trade. The second component gives all the bargaining power in renegotiation to the other party (say the buyer), by allowing that party to make a take-it-or-leave-it offer. The timing of the renegotiation game is as follows: (1) the parties make investment decisions, (2) the buyer makes a take-it-or-leave-it offer, and (3) the seller can accept the offer (in which case trade takes place on those terms) or can trigger the default trade. This two-stage mechanism achieves the

[32] This is reflected in a number of Nobel Prizes related to this literate. After Ronald Coase won the prize for his transaction cost theory of firm size, Oliver Williamson won it in 2009 in large part for his work on holdup. Jean Tirole won in 2014 for a range of contributions, one of which was his work on renegotiation design mechanisms. Finally, Oliver Hart just won the prize in 2016 for explaining how asset ownership and residual rights of control can promote efficient ex ante investment and thus provide a theory of vertical and lateral integration.

socially optimal level of investment by both parties. To see why, note that the seller, despite having no bargaining power at the take-it-or-leave-it stage, is the residual claimant on her investment due to her access to the default option in the second stage of the game, and thus has appropriate incentives to invest optimally. Inducting back to the take-it-or-leave-it-stage, the buyer, because it has all the bargaining power, has the requisite incentives to invest optimally.[33]

To see how this renegotiation game plays out in the Apple-Corning example,[34] there is a single unit of glass to be traded, so it is convenient to think of setting the default probability that a widget will be traded. The first component of the ADR mechanism is the default trade that Corning can trigger. We set the default probability of trade at 5/6 and the default price at $23 1/3. We will not go through a derivation of the numbers we have chosen here,[35] but they are constructed to do two things: split the ex-ante surplus evenly between Apple and Corning, and ensure that Corning has the appropriate incentives to make the cost-reducing investment. The second component of the ADR mechanism is to give Apple the right to make a take-it-or-leave-it offer.

What is the best offer for Apple to make when they get the opportunity? Since Apple is making a take-it-or-leave-it offer they have all the bargaining power and will thus want to trade the efficient amount of glass, which here is one unit. Apple, possessing all the bargaining power, will extract Corning's entire surplus. This leaves Corning indifferent between the default option and accepting Apple's offer. Corning will thus anticipate getting the same payoff as under the default option, whatever happens.

Now work backwards, and consider Corning's decision whether to invest at the earlier stage. If Corning invests they get a payoff equal to $23 1/3 − (5/6) × $10 − $5 = $10 (the price minus probability of trade multiplied by the cost of production, minus the investment cost). If Corning does not invest they get a payoff equal to $23 1/3 − (5/6) × $16 = $10. So, Corning is willing to invest.[36]

Now consider Apple, who is the residual claimant on their investment. They obtain $8 if they make the investment, but bear a cost of just $5. So, Apple also makes the efficient investment. Thus, total surplus is $40 − $10 − $5 − $5 = $20. Remarkably, this is the first best—the same as if Apple and Corning could contract on all relevant contingencies.

It is, at first glance, rather surprising that Corning finds it optimal to invest despite having none of the bargaining power in the renegotiation. The key is their ability to reject Apple's offer and trigger trade under the terms of the default option. The default option becomes more appealing when the glass is low cost, which happens precisely when Corning invests. In other words, the presence of the default option makes Corning's payoff sensitive to their investment.

---

[33] See Aghion et al., *supra* note 18, at 263-266.

[34] This description is based heavily on Holden and Malani, *supra* note 6, at 162-164.

[35] A general derivation is as follows. Suppose that the valuation, v, to the buyer is either v_L or v_H and the seller's cost of production is either c_L or c_H. Trade takes place at price p. The buyer can invest j at cost $\phi(j)$ which makes the probability of the high valuation equal to j. Similarly, the seller can invest amount i at cost $\phi(i)$ which leads to the probability of the low-cost state being i. The buyer's payoff is thus $vq - p - \phi(j)$, and the sellers is $p - cq - \phi(\mathrm{i})$. Let the default option be a price quantity pair $(\tilde{p}, \tilde{q})$. Set the default level of trade such that $\tilde{q}(c_H - c_L) = \phi'(i^{FB})$, where the superscript FB denotes the first-best level of investment. The default price is set to split the surplus according the respective bargaining weights of the two parties.

[36] It is easy to break the indifference slightly in favor of investing without altering the analysis.

C. Mechanisms to address non-verifiability more generally

So far, we have examined the problem of hold-up when the parties make relationship-specific investments, like Alaska Packer's chartering of a ship to take plaintiff fishermen to Alaska, or in our Apple and Corning example. However, there may be important ex-post inefficiencies that arise from the inability to write complete, state-contingent contracts even in the absence of relationship-specific investments.

The economics literature has only recently made progress in providing formal models of such ex-post inefficiencies, typically through the use of ingredients from social psychology such as "reference points".[37] We will not delve into those formal models here. However, we do highlight solutions to these ex-post inefficiencies that do not restructure renegotiation so much as get the parties to truthfully report non-verifiable information to the court, making that information verifiable.

Beginning with Professor Maskin (1977),[38] a large literature has explored how carefully crafted mechanisms that require players to make announcements, and face payoffs dependent on those announcements, may be able to cause information observable to players but not to outsiders to *become* observable and thus verifiable by outsiders. This is particularly useful in the hold-up setting because once the parties know that the true state will be revealed then, then they can *ex ante* contract on v or c, even if they cannot contract on relationship specific investments per se.[39]

An illustration of Professor Maskin's theorem in the Apple-Corning setting is as follows. To make Apple's value v – which both Apple and Corning know once it is realized – verifiable to a court, each party is asked to simultaneously announce 40 or 32. The mechanism specifies that if both parties agree in their announcement then that is the stipulated value of v. If the parties disagree then each pays a very large fine to a third party.

It is straightforward to see that both Apple and Corning announcing truthfully is a Nash equilibrium. Suppose v is actually 40. Conditional on Apple announcing "40", the Corning's best response is to announce "40" as they avoid the large fine. Unfortunately, both parties not announcing truthfully is also a Nash equilibrium. Suppose again that v is actually 40. Conditional on Apple announcing "32" the best response of Corning is to announce "32" to avoid the fine.

Troubled by this multiplicity of equilibrium, Moore and Repullo (1988) show that by using a multi-stage mechanism it is possible to implement any social objective as the unique (subgame-perfect) equilibrium of the game induced by that mechanism.[40] The following, based heavily on Aghion and Holden (2011),[41]

---

[37] See, notably, Oliver Hart & John Moore, Contracts as Reference Points, 123 THE QUARTERLY JOURNAL OF ECONOMICS 1 (2008).

[38] Eric Maskin, Nash Equilibrium and Welfare Optimality, mimeo (1977), ultimately published as Eric Maskin, Nash Equilibrium and Welfare Optimality, 66 THE REVIEW OF ECONOMIC STUDIES 23 (1999).

[39] For example, they can limit how much p rises when v is high or p falls when c is low so as to ensure each party has adequate incentives to invest in raising v or lowering c.

[40] John Moore & Rafael Repullo, Subgame Perfect Implementation, 56 ECONOMETRICA 1191, 1208, 1212 (1988).

[41] See also Moore & Repullo, *supra* note 40, at 1196.

is an example of this kind of mechanism in the context of the Apple-Corning example we have been using.

1. A(pple) announces either 40 or 32. If the announcement is 40 then A pays C(orning) a price equal to 40 and the mechanism stops.
2. If A announces "32" and C does not challenge A's announcement then A pays a price of 32 and the mechanism stops.
3. If C challenges A's announcement then
    a. A pays a fine of 30 to a T(hird party)
    b. A is offered the glass for 22
    c. If A accepts then C gets 30 from T (and 22 from A for the glass)
    d. If A rejects the glass then C pays 30 to T
    e. A and C Nash bargain over the glass.

We will not go through how to establish that truth-telling is the unique equilibrium here, but refer the interested reader to Aghion and Holden (2011) for the requisite logic, though with different numerical values.[42]

D. Information problems

Rarely, if ever, are the renegotiation design or the revelation mechanisms described above seen in practice. This begs the question: why not? One reason may be that these mechanisms seem too complex to implement as they require two or three stages of structured bargaining. Holden and Malani show that these hurdles cannot be too large because, while uncommon, procedures like the ADR mechanism can be found in, e.g., variable quantity contracts.[43] Moreover, even the multi-stage procedures in Moore-Repullo mechanisms are less complicated than some arbitration procedures to which contractual parties agree, let alone actual trials and the civil procedure rules that govern contracts in the absence of arbitration provisions.

1. Uncertainty

Another explanation for why the aforementioned mechanisms are uncommon is the substantial information requirements of these mechanisms. One piece of information required is that the parties need to know the cost and payoffs to each type of investment to employ these mechanisms. For example, both parties must know the cost of the Corning's investment ($5) and the amount that it will reduce costs c (from $16 to $10) in order to set the default option (trade of 5/16 a unit for $23 1/3). Often these numbers are uncertain. In that case, the parties cannot precisely structure the mechanism, which in turn means that the mechanism may not always deter holdup.

[42] Philippe Aghion & Richard Holden, Incomplete Contracts and the Theory of the Firm: What Have We Learned over the Past 25 Years?, 25 JOURNAL OF ECONOMIC PERSPECTIVES 181, 191 (2011).
[43] Holden and Malani, *supra* note 6, at 155.

If this sort of uncertainty looms large, the parties can only avoid renegotiation by foregoing renegotiation of their original contract altogether. We will discuss how this might be achieved without and with blockchain in Sections III and V, respectively. The downside of this approach is that parties lack the flexibility to renegotiate where there is no hold-up but there are changed circumstances such that both parties would benefit from a different bargain than the original contract.

2. Information asymmetry

A different sort of problem arises if there is information asymmetry between the parties. Professors Aghion, Fudenberg, Holden, Kunimoto and Tercieux (2012) argue, theoretically, that complex mechanisms are not robust to small perturbations from common knowledge.[44] We will not go into the intricate details of their logic here, but their claim hinges on the observation that the above mechanisms implicitly assume not just that the state of nature is observable to the contracting parties, but that it is also *common knowledge* among the contracting parties. In other words, the mechanisms assume that Apple and Corning not only observe v and c, but agree on what v and c are.[45]

Aghion et al. then show that these mechanisms are not robust to an arbitrarily small perturbation away from common knowledge, i.e., to Apple and Corning honestly disagreeing even slightly about the value of v or c. In this context, two-stage renegotiation-design mechanisms like ADR may yield optimal trade and thus investment, but they may also yield equilibria with suboptimal trade and investment. In other words, investment is not the unique equilibrium of those mechanisms.[46]

Things get worse with more complicated, three-stage mechanisms such as that of Moore and Repullo.[47] With those, arbitrarily small deviations from common knowledge causes not just the emergence of non-truth telling as an equilibrium, it causes truth-telling to no longer be an equilibrium. In other words, the parties cannot even contract on v and c because they will never be truthfully revealed.[48]

Experimental evidence from Aghion, Fehr, Holden and Wilkening (2017) supports this theoretical finding with respect to revelation mechanisms in particular, but also offers some hope. They show that revelation mechanisms underperform due to asymmetric information, but that the degree of underperformance is proportional to degree of asymmetric information.[49] In other words, the less the information asymmetry, the better the performance of revelation mechanisms, even though they do not achieve perfect truthfulness and thus maximal investment incentives.

---

[44] Philippe Aghion, et al., Subgame-perfect implementation under information perturbations, 127 THE QUARTERLY JOURNAL OF ECONOMICS 1843 (2012).

[45] It may seem strange that both Apple and Corning can observe v and c bot not see the same thing. The reason that both may get some information on v and c that is unbiased, but not precise. I.e., they see v and c plus some random noise. In that context, the two parties get equal quality information on v and c, but not agree on v or c.

[4646] Aghion et al., *supra* note 44, at 1870, 1875.

[47] Aghion et al., *supra* note 44, at 1863.

[48] The reason for the more dismal result with three stage mechanisms is that the party that plays in the second stage not only has no incentive to tell the truth, but has an incentive to lie, because the other party gets to play again after her. With two stage mechanisms, player 2 does not have to worry about what player 1 will do after she moves.

[49] Philippe Aghion, et al., The Role of Bounded Rationality and Imperfect Information in Subgame Perfect Implementation—An Empirical Investigation, JOURNAL OF THE EUROPEAN ECONOMIC ASSOCIATION 1, 27 (2017).

III. PRACTICAL SOLUTIONS TO THE HOLD-UP PROBLEM BEFORE SMART CONTRACTS AND BLOCKCHAIN

There are a number of ways that parties and courts can, in practice, address the problem of hold-up, though each approach has its shortcomings.

A. Private solutions

Ideally, the parties would write a contract that precisely specified what investments each party would make in each state of the world and at what price and quantity they would trade given the result of those investments. Economists call this a complete state-contingent contract that specifies the parties' payoffs in all states of the world. In this context, courts would have no reason to allow renegotiation -- correctly or mistakenly – because the original contract would account for all possible changed circumstances. That, in turn, would deter holdup.

Yet such contracts are nearly impossible to write. Parties may not know all possible states or it may not be cost effective to specify them all ex ante. Moreover, courts often cannot verify what state the parties are in and thus enforce the appropriate contractual provision.[50] Indeed, this is the reason that the starting assumption of the economic literature on the hold-up problem is that parties cannot and do not write, or courts cannot enforce, complete contracts.[51]

One alternative solution is for the two contracting parties to merge and conduct the transaction internally within a single firm. This option is why Professor Coase and later Professor Hart predicted that holdup could provide incentives for the parties to move their transaction from the market, mediated by contract between firms, to organizing the transaction within a single, integrated firm.

While Apple and Corning integrating[52] would address the glass plate supply problem, both parties also deal with other suppliers and purchasers. Corning cannot both integrate with Apple and with, say, Motorola, another smartphone OEM. As a result, integrating with Apple would mean having a less efficient relationship with Motorola, due to holdup. Nor would Apple want to own every single one of its thousands of suppliers, even though their deals may also entail hold-up risks. Managing all those relationships internally within a firm simply replaces hold-up problems with internal agency problems.

---

[50] See *supra* text accompanying note 12.

[51] See Oliver Hart & John Moore, Property Rights and the Nature of the Firm, 98 JOURNAL OF POLITICAL ECONOMY 1119, 1126 (1990); Aghion and Holden, *supra* note 42, at 182.

[52] We use the term integrating rather than merging here because the term merger may mean something to the contract theory literature than it means in the legal literature. Scholars in the contract theory literature sometimes worry that merger implies takeover of one firm by another, which is not a necessary condition to obtain the results of operating under the roof of one firm. The legal literature does not treat merger as the same as acquisition, as indicated by their use of the term "mergers and acquisition" rather than simply "mergers" to describe corporate law rules pertaining to the transformation of two firms into one. The implication for the legal audience is that we could substitute the term merger for integration in the main text if our only audience were legal scholars.

A second alternative for the parties is to rely on repeat play and reputation. If Apple and Corning transact each year for each new iteration of Apple's smartphone, they each have a strong incentive not to hold the other up, lest they jeopardize future deals between them.[53] That said, if the power to hold up is asymmetric, it would affect the aggregate division of gains from trade across all the parties' contracts in favor of the party with more hold-up power. This in turn could reduce the incentive of the weaker party to participate even in repeat play transactions. More importantly, many parties do not transact repeatedly – or expect that their repeated transactions will one day end.[54] In that context parties must rely on market reputation.[55] The challenge is that, if courts cannot verify holdup, other companies may might not be able to either.

A third alternative is for the parties to employ one of the renegotiation design or revelation mechanisms discussed in Section II. For instance, they could specify default trades that favor on party and give the other party the right to make a take-it-or-leave-it offer as the ADR mechanisms suggests,[56] or they could specify alternating price announcements and challenges alongside payments to third parties as the Moore-Repullo mechanism proposes.[57]

The weakness of these mechanisms is that they each require a strong form of commitment, which is a significant barrier to their usefulness. If the weaker party can refuse the take-it-or-leave-it offer and the stronger party would still trade (which it is mutually rational to do), then the ultimatum is not credible and it will not give the stronger party adequate return on its investment. Likewise, if the parties agree to split the penalty payment to the third party rather than hand it over to that party (again which is mutually rational to do), then the parties do not have an incentive to truthfully announce their valuations prior to the penalty round. Yet it is unlikely that the parties can credibly commitment to actions required for renegotiation design or revelation mechanisms if they cannot make such commitments to the original contract to deter holdup in the first place.

One way to obtain this commitment, ostensibly without smart contracts and blockchain, is to include penalty clauses – liquidated damages larger than economic damages – if the parties do not comply with the mechanisms.[58] For example, the stronger party may have to pay a penalty if it makes a second offer after its take-it-or-leave-it offer is rejected by the weaker party but before the weaker party requests the default trade in the ADR mechanism.[59] Indeed, penalty clauses could go further and possibly dis-

[53] See Klein et al., *supra* note 18, at 302 (explaining the value of long term contracts).

[54] With finite period games, the parties have an incentive to hold-up in the last stage. Given they have that incentive in the last stage, they will also have it in the penultimate stage, which now looks like the final stage. This process repeats until the value of repeat play evaporates. Robert Gibbons, GAME THEORY FOR APPLIED ECONOMISTS 82 (1992).

[55] In our usage, reputation differs from repeat play because it can rely on shirking – in this case by holding-up – being revealed to other parties that contract with the shirking party, reducing the latter's gains from trade with other parties. This distinction between repeat play (sometimes called trust) and reputation is somewhat different than the usual distinction between these concepts in the economics literature. The latter distinction relates repeat play to hidden action and reputation to hidden type.

[56] Aghion, et al., *supra* note 18, at 258.

[57] See Moore and Repullo, *supra* note 40, at 1196.

[58] See Gerrit De Geest & Filip Wuyts, Penalty clauses 141, in ENCYCLOPEDIA OF LAW AND ECONOMICS. 3: THE REGULATION OF CONTRACTS (2000).

[59] In some cases, the penalty clause may have to be paid to a third party, otherwise it might directly undermine the incentives the mechanism set up for the parties. For example, if the penalty for negotiating around the third party

incentivize holdup in the first place by penalizing deviations from the original contract terms, if the parties are comfortable with foregoing any flexibility to depart from the original contract.

The problem with this approach is that courts frown upon penalty clauses, though they may be more permissive in cases where both parties are sophisticated businesses rather than cases involving small businesses or individual consumers.[60] If courts won't enforce the penalty clause, it will not incent parties to commit to their roles in the mechanisms or to their original contract terms.

Even if courts would enforce the penalty clause, it can skew the incentives of the two parties. Such clauses act like reliance damages, which are known to risk overinvestment by the protected parties.[61] The solution to overinvestment is to pay the penalties to a third party rather than the party making an investment.[62] Yet both contractual parties have a mutual incentive to negotiate around that third-party payment, as they did in the revelation mechanism.[63]

The only way to obtain commitment without skewing investment incentives then is to have an automatic payment to a third party that cannot be undone by the contractual parties. For example, the parties could set up something akin to a poison pill where the contract or mechanism creates an IOU from the penalized party to a third party.[64] Of course, if there is a gap between the timing of the investment and the payment for that investment, the holding-up party could still petition a court to enjoin the poison pill-type penalty before it is triggered by failure to make payment for the investment. The held-up party is unlikely to invest much to stop the holding up party because it does not benefit from the payment to a third party.

To avoid both circumvention of the penalty by the parties (directly) and by courts (after being petitioned by the parties) is to have the penalty be something that even the court cannot enjoin. An outlandish but effective solution is to create a machine, have the party that needs to show commitment place a large amount of cash in the machine, then have the machine rigged to burn the cash if that party fails to meet its commitment. The machine must have a dead hand switch so that it is triggered if anyone – even the court via injunction – tries to shut it down.

This machine must be all-knowing about the parties' accounts, otherwise the parties could get around even this machine. Specifically, they could renegotiate but transact in two parts: one that appears to the machine to conform to the original contract and a second that undoes the original contract and consummates the renegotiated contract. If the machine only observed the first transaction, it would release the cash it was holding hostage even though the second transaction consummated the renegotiated contract. Again, investment incentives would be undermined.

---

payment in the revelation mechanism is a penalty paid by one of the parties to another, they would simply account for it in their negotiations over the first payment.

[60] EDWARD ALLAN FARNSWORTH, FARNSWORTH ON CONTRACTS 845 (Aspen Publishers. 2003).

[61] William P. Rogerson, Efficient Reliance and Damage Measures for Breach of Contract, 15 THE RAND JOURNAL OF ECONOMICS 39, 41 (1984).

[62] See Holmstrom, *supra* note 18, at 327 (showing that relaxing the budget breaker yields an efficient Nash equilibrium of the moral hazard in team game).

[63] Id.

[64] Suzanne S. Dawson, et al., Poison Pill Defensive Measures, 42 THE BUSINESS LAWYER 423 (1987).

But this machine we have described is hard to build and actually looks very much like a smart contract on blockchain. Moreover, the latter are simple and cheaper to implement. The smart contract is just a computer script not an awkward physical machine; it can work with digital money, which is easier to obtain than actual cash; and can be made all knowing with APIs to all the parties accounts.[65] Moreover, blockchain allows irreversible transfers to anonymous accounts.

B. Public solutions

Perhaps courts could help parties avoid holdup. One idea would be for courts to ban renegotiation completely. This solution goes too far as it would bar renegotiation due to truly changed circumstances, even if both parties wanted it. Alternatively, courts could try to distinguish cases where renegotiation was due to holdup rather than changed circumstance or they could only enforce renegotiated contracts if the original contract contained provisions allowing renegotiation. The former idea is actually the current rule: we already saw in *Alaska Packers* that courts may not have enough information to get the correct answer to whether there was hold-up.[66] As for the latter idea, it is itself subject to holdup. If parties sign a contract requiring no renegotiation, the party committing the holdup would simply renegotiate to have the held-up party settle the original contract breach case at a low price and then sign a renegotiated contract. Perhaps the transfer to the holding-up party would be smaller, but it would not eliminate the whole hold-up problem.

IV. BACKGROUND ON BLOCKCHAIN AND SMART CONTRACTS

We believe blockchain technology, used together with smart contracts, can overcome some of hurdles to credible commitment in contracts with current contracting technology. In this section, we describe the main value added from blockchain and smart contracts and then explain how these technologies might better enable the sort of contractual commitment required either to stop all renegotiation or to enable the use of renegotiation design or revelation mechanisms, the two strategies for eliminating holdup.

A. The value of blockchain

Blockchain, a computer science innovation introduced by Satoshi Nakamoto in 2008, is described as a distributed or decentralized, open and secure ledger, meaning it that verifies transactions are intended, feasible and executed through a decentralized system rather than through a central authority (like a government or bank, which might be costly or untrustworthy), records transactions in a public way (so as to build reputations and counterparty trust), and ensures transaction are not reversible (to protect parties from certain types of theft).[67] Although Nakamoto initially intended the term transaction to

[65] See infra Section V

[66] See Posner, *supra* note 11, at 46; Chirelstein, *supra* note 11, at 65.

[67] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system 1, White Paper (2008). Nakamoto is a pseudonym; his or her identity is uncertain. See Satoshi Nakamoto, WIKIPEDIA, available at https://en.wikipedia.org/wiki/Satoshi_Nakamoto (last visited on December 20, 2017).

mean a monetary transfer, a transaction recorded in the blockchain can be any set of promises, i.e., a contract, or indeed any statement.[68]

1. The core function of blockchain is witnessing statements (without relying on any one witness)

A simple analogy clarifies the core function of Blockchain. Blockchain – which refers both to the method by which a record of statements is made and to the recorded statements themselves – is akin to a witness. Suppose A and B agree that A will rent an apartment to B for $600 per month. We can decompose that agreement into a statement by A that A will give B access to the apartment and by B that B will pay A a given amount per month. To commemorate their transaction, they can each write down these statements on paper and sign those statements. The written statements can serve as proof to third parties that A and B made the statements written down. An alternative is to find a witness. If that witness is a neutral third party, then she can testify credibly to outsiders that the statements that A and B make. Either way, outsiders would be able to more confidently rely on statements from B that she has an apartment she wants to rent out, or from A that he has $600 to spend.[69]

A witness's value – relative to paper statements – is not that they are uniquely credible, but that they incrementally improve the credibility of statements and in some cases more cost-effectively enhance such credibility. Certainly, a paper document plus a witness is more credible than just a paper document. Witnesses may also have two advantages over paper documents. In some cases, the witness may be cheaper, because paper documents may require the assistance of costly lawyers to write. The witness also may be more credible, because a paper contract can sometimes be forged. This is not always true: a witness may lie if they are biased in favor of or bribed by one of the parties. But the witness may be better than paper documents in some cases.

Blockchain is simply a new technology to witness transactions. The old-fashioned approach is to have another human, ideally unrelated (or equally related) to the two or more parties to a transaction, observe the transaction. In some cases, it was a central, privileged party, such as the government, e.g., when a judge witnesses a wedding, or a bank, which might validate a check from B to A. In other cases it was simply an authorized third party, e.g., a public notary. In yet other cases, the witnessing is recognized ex post, as required, as when a court admits as probative evidence such as a document that was signed by both parties. Blockchain's approach to witnessing is different: it uses cryptographic algorithms mediated by a computer network.

At its base, blockchain sets up a network. Two of the more popular such networks are Bitcoin and Ethereum.[70] If A and B want to transact, they each announce their transaction to the network. Blockchain sets up a method by which computers on the network, called "nodes," can hear the

[68] Vitalik Buterin, A next-generation smart contract and decentralized application platform 14, White Paper (2014).
[69] One notable outsider is a court: if there is a dispute over the agreement and the parties go to court, the witness can help the court resolve issues of fact.
[70] Bitinfocharts, Bitcoin, Ethereum Transactions historical chart (last visited on Oct. 2, 2017), available at https://bitinfocharts.com/comparison/transactions-btc-eth.html#3m (showing that Bitcoin and Ethereum have equal volume, greater than other cryptocurrency platforms).

messages from A and B. The nodes then produce evidence that they heard that message, i.e., they validate it.[71]

Technically speaking, the evidence that validates a transaction on a blockchain network is the output from a so-called "hash function", a type of one-way function in mathematics.[72] A hash function is an algorithm wherein, upon hearing what A and B say, the node – call her W as it serves as a witness – transforms the message into a "hash". (The action of transforming the message is called 'hashing'). The key feature of the hash is that people who observe it know that W must have witnessed A and B saying they were going give access to an apartment and pay $600/month, respectively. How do they know that? Because hash functions have the property that there is no way for W to produce its hash unless its heard A and B say they were going to give access to an apartment and pay $600/month, respectively. In other words, one of the inputs to the hash function is the announced transaction and the output is a hash that validates that the transaction was indeed announced.[73]

Once the network produces evidence of a transaction, i.e., the hash, it is added to a list of previously witnessed transactions. The whole list is called the blockchain, so sometimes people say they "add the hash to the blockchain".[74] Because the blockchain is a list of transactions, it is also called a ledger.[75]

Knowing that blockchain is analogous to having a witness publicly validate statements, one can determine when blockchain is valuable and when it is not. These considerations explain a number of specific technical details about blockchain. Because these are not directly relevant to the main argument of this paper, we relegate a description of those consideration to Appendix II.

2. Blockchain is an open ledger to take advantage of the economies of scale from witnessing

---

[71] Nakamoto, *supra* note 67, at 2. See also Bitcoin.org, Bitcoin Developers Guide (last visited on Oct. 2, 2017), available at https://bitcoin.org/en/developer-guide#block-chain.

[72] Id. A one-way function is a function where if you know the inputs, you can produce the outputs, but if you only have the outputs, you cannot know for sure the inputs. Andreas M. Antonopolous, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN 2ND EDITION 56 (2017). An example is 2 + 3 = 5. The inputs are 2 and 3 and the function is addition. The output is 5. If you know 2 and 3, you know the output of addition is 5. But if you know only 5, you cannot know whether the inputs are 2 and 3 or any of the following pairs: (0,5), (5,0), (1,4), (4,1), (3,2).

Addition is not the best one-way function for blockchain, as it is also desirable to have a situation where only when A and B present 2 and 3 can they prove that were the ones that spoke. With addition, A and B could come forward and say they said 1 and 4, and it too would be validated since the sum is 5. So, the one-way functions are both a one-way and unique mapping from inputs to outputs. A better example than addition is prime factorization, which is actually used in cryptography. If I give you a number X and ask you the fewest number of primes that, when multiplied together, yield X, you have a problem that rises quickly in complexity as X increases. If I tell you a series of primes, you can easy calculate its product X; but if I just give you X, it is very difficult to calculate its prime factorization.

A forme of one-way functions used often with blockchain are trap-door functions. These are one-way functions such that, if you have some secret information (i.e., know the "trap-door") you can compute the inputs form the outputs.

[73] Id at 227-228.

[74] Nakamoto, *supra* note 67, at 2; Bitcoing.org, Bitcoin Developer Guide, *supra* note 67.

[75] Antonopolous, *supra* note 72, at 2. See also, e.g., Blockgeeks.com, What is Blockchain Technology? A Step-by-Step Guide For Beginners: An in-depth guide by BlockGeeks, available at https://blockgeeks.com/guides/what-is-blockchain-technology/ (last visited on Oct. 2, 2017).

Blockchain is often described as a public, distributed ledger. The distributed portion refers to the method of witnessing, which we just described. But the open ledger portion of this refers to the fact that the blockchain is publicly available.[76] The reason it is open is that there are economies of scale from witnessing.

By economies of scale in witnessing, we mean that the value of witnessing two transactions is worth more than witnessing just one transaction. To see why that is, consider our rental transaction: A gives B rights to an apartment and B gives A $600 per month. Suppose C wants to sublease the apartment. If C is able to observe that A gave B rights to the apartment, C is more confident that B has rights to the apartment C wants. Of course, the fact that potential counterparties benefit from observing A and B's exchange just means that witnessing A and B's exchange is valuable. To show economies we must show that D, who wants to use the apartment C has for a weekend in an Airbnb-type transaction, benefits not only from seeing B's transfer to C, but also A's transfer to B. That is certainly the case: seeing A give B the apartment gives D confidence that B had an apartment to give to C. In other words, being able to observe multiple transactions increases a party's confidence that their counterparty actually has the asset that is to be transferred to the party. There are economies because once A and B's transaction is observed and publicly validated on the blockchain, it can be used both by C and, without additional cost, by D.[77]

A necessary condition for witnessing to have economies of scale is that the validation be made public and that ownership be traceable across transactions. To reduce transactions costs, the public validation should be maintained in a database where public validation of other related transactions is maintained. So, the feature of blockchain that achieves these economies of scale is that it is publicly searchable.[78]

Earlier we said that the core function of blockchain is witnessing rather than public reporting. We said that in part because blockchain without witnessing is just an open database, like the title registry that tracks land ownership. It is witnessing that gives entries into the database value. In the last section, we noted blockchain is an open database.

3. Security and the inalterability of blockchain

A feature that distinguishes a blockchain public database of transactions from other public databases of transactions is that there are so-called consensus rules. With a traditional database, a central authority is charged with making sure the database is not retroactively modified to reallocate ownership of items. If the centralized authority is untrustworthy, e.g., if it is also a participant in transactions recorded on the database or it might accept side payments from participants to modify the database, then the database's credibility is compromised.[79] With a blockchain database, there need not be any central administrator of the database. Anyone can contribute an entry. But what stops anyone from also modifying old transactions (perhaps to benefit themselves or harm competitors)? Each blockchain

[76] Marco Iansiti & Karim R Lakhani, The Truth About Blockchain, 95 HARVARD BUSINESS REVIEW 2, 5 (2017).
[77] Of course, there is a marginal cost to D of processing the information about A and D. We ignore this as that cost is the same regardless of how the information about A and B are generated.
[78] Antonopolous, *supra* note 72, at 16, 147.
[79] Id at 217.

network has a consensus rule that determines when a database can be updated and therefore also retroactively modified.[80]

The most common consensus rule is proof-of-work validation, in which nodes compete to be the first to hash an announced transaction and the winner is the first to add the transaction to the blockchain.[81] This method requires a node to deploy CPU time (i.e., electricity and a CPU) to perform hash functions and thereby validate transactions. To change a past transaction, a node has to employ enough CPU time to modify an old transaction and revalidate all other transactions, including new transactions that are occurring in the interim. This requires a lot more CPU time; indeed, Nakamoto showed that it requires that no one node controls a majority of all CPU power on the blockchain network.[82]

Although proof-of-work makes retroactive modification of the blockchain hard, it also makes validation of new transactions hard. By hard we mean it consumes a lot of electricity.[83] An important alternative method being explored is proof-of-stake. Under proof-of-stake, transactions are validated by betting that they are correct. Nodes put up money that the transaction they state occurred actually occurred. If others put up more money that the transaction did not occur, then the node betting on the transaction loses the money that the transaction occurred.[84] Other alternatives include other methods of voting for which transaction actually occurred, with the alternatives being differentiated by the weight that each node's vote has.[85] With alternatives to proof-of-work, the manner in which transactions are validated should be chosen so as to balance the goal of reducing the cost of incentives to validate truthful transactions and of increasing the cost of incentives to retroactively modify past recorded transactions.[86]

4. Anonymity and privacy on the blockchain

Another feature that makes blockchain attractive to some[87] is that blockchain can preserve anonymity or promote privacy. This is done in either of two ways. One is by disassociating accounts with personal identities on the blockchain database. For example, people may just have public identification numbers, also called public keys, and those keys are not associated with names, addresses or other identification numbers easily connected to names or addresses.[88] It should be noted, however, that various governments have imposed know-your-customer (KYC) rules on exchanges that facilitate transactions on

[80] Id at 26.
[81] Nakamoto, *supra* note 67, at 3. For more detail, see Bitcoing.org, Bitcoin Developer Guide, *supra* note 67.
[82] Nakamoto, *supra* note 67, at 6-7.
[83] See Vitalik Buterin, A Proof of Stake Design Philosophy, MEDIUM (Dec. 30, 2016), available at https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51 (last visited on Oct. 2, 2017).
[84] Id.
[85] See Amy Castor, A (Short) Guide to Blockchain Consensus Protocols, COINDESK (March 14, 2017), available at https://www.coindesk.com/short-guide-blockchain-consensus-protocols/ (last visited on Oct. 2, 2017). For a more technical description, see Arati Baliga, Understanding Blockchain Consensus Models 7-10 (whitepaper), April 2017, available at https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf?pdf=Understanding-Blockchain-Consensus-Models (last visited on Oct. 2, 2017).
[86] Id at 5.
[87] This includes individuals trading in illegal goods, such as the seller on the Silk Road website, individuals facing capital controls, as well as individuals facing the risk of expropriation by governments or instability in their countries.
[88] Antonopolous, *supra* note 72, at 57.

blockchains and these can make it harder to maintain anonymity on the blockchain.[89] A second way to ensure privacy is to create and maintain a private blockchain that is only accessible to a small number of participants or that can only be searched by a centralized intermediary, who can validate whether counterparties have certain assets or not.[90]

Both methods of limiting public knowledge of transactions, unsurprisingly, limit the economies of scale from blockchain. As a result, blockchain networks must balance the returns to scale with the value of privacy when choosing how they will be constructed.

B. The value of smart contracts

So-called smart contracts, as first conceived by Nick Szabo,[91] are a quite general concept: a smart contract is a simply series of actions written in computer script.[92] When the actions constitute fulfillment of mutual, conditional promises, they are a contract in the traditional sense.[93] Smart contracts can fully or partially specify a contract, meaning they can include all promises made pursuant to a contract or they can contain part of the promises, in which case the code plus a paper agreement constitute the whole contract.[94]

Smart contracts can exist independent of a blockchain network, but they can also be announced, witnessed and automatically executed on such a network. Indeed, the reason Vitalik Buterin created the Ethereum network was that the Bitcoin network did not support smart contracts. Ethereum is a blockchain network but with a scripting language that allows smart contracts. Individuals write their smart contracts in that script and the Ethereum network validates and executes it.[95]

1. Benefits that smart contracts do <u>not</u> offer

What makes smart contracts special is not that they are automated. One can already automate transactions. Take the case where A rents and apartment to B for $600/month. With a smart contract,

---

[89] See, e.g., Joshua Althauser, Australian Government Moves to Regulate Cryptocurrency Exchanges, COINTELEGRAPH (Aug. 18, 2017), available at https://cointelegraph.com/news/australian-government-moves-to-regulate-cryptocurrency-exchanges (last visited on Oct. 2, 2017).

[90] Tiana Laurence, BLOCKCHAIN FOR DUMMIES 8 (For Dummies 2017).

[91] Nick Szabo, Smart Contracts: Building Blocks for Digital Market, Entropy #16, available at http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

[92] An example of a scripted contract on the Ethereum network is available at https://www.ethereum.org/token (last visited on Oct. 2, 2017).

[93] Indeed, smart contracts can be used to create not only real-world contracts but also real world corporations. One of the original smart contracts on the Ethereum network was the decentralized autonomous organization (DAO). A DAO is a set of smart contracts that specify the governance, assets and liabilities of a group of people or nodes on a network. Ian Allison, Ethereum reinvents companies with launch of The DAO, Apr. 30, 2016, available at http://www.ibtimes.co.uk/ethereum-reinvents-companies-launch-dao-1557576.

[94] Josh Stark, Making Sense of Blockchain Smart Contracts, COINDESK (June 4, 2016), available at https://www.coindesk.com/making-sense-smart-contracts/ (last visited on Oct. 2, 2017).

[95] Vitalik Buterin, A Next Generation Smart Contract & Decentralized Application Platform: Ethereum Whitepaper 13 (2014), available at http://www.the-blockchain.com/docs/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (last visited on Oct. 2, 2017).

simply by signing the contract B would automate the process of paying A because her account on the blockchain network would be deducted $600 per month. But B could have done that before smart contracts. For example, she could have signed a paper rental agreement and then set up a standing order at her bank to send A an e-check for $600 each month.[96]

Of course, there are fewer steps with a smart contract, which could reduce transactions costs with contract execution. Writing and digitally signing a smart contract script could, in theory, eliminate the need to take extra steps to automate the process.[97]

But this benefit is offset by the fact that automation via smart contract requires the smart contract to be on a network that controls enough of A and B's assets to be able to be completely self-executing on that network. For example, if B writes her smart contract on the Ethereum network but does not have her wealth in an Ethereum network account, then she would have to transfer money to an Ethereum account to empower Ethereum to direct it according to the contract. If all B did was to allow an Ethereum network to check her regular bank account, the smart contract could not execute her contract.

Nor do smart contracts obviously reduce transactions costs during contract drafting. Traditional contracts require the parties and/or a lawyer to draft a contract. But smart contracts require the parties and/or a hired programmer to script those contracts. Services like Legal Zoom can help with form contracts, but form contracts can be used to economize with traditional paper contracts as well as script contracts.[98]

So, what are the benefits of smart contracts over ordinary contracts?

2. Smart contracts reduce uncertainty about promises (counterparty risk)

A smart contract, by virtue of being a plan for the future and being automated, gives counterparties confidence that promises will be fulfilled. Take our rental example. Even if B sets up an automatic payment for $600/month to A with her bank, there is a risk that the payment will not be made. To see why, suppose B only has $600 in her account on September 29 and rent is due October 1. If B decides to have dinner out on the 29th that costs $25, her bank will not be able to transfer $600 on the 1st. She will be $25 short. By contrast, a smart contract can be written so that her account encumbers the $600 even before the 1st due so that B cannot spend $25 on dinner on the 29th if she only has $600 in her account that day.[99]

An inexact analogy to the smart contract counterparty is a secured creditor. A secured creditor knows that, even if the debtor cannot pay her debts even after litigation or bankruptcy, the creditor can seize their collateral, e.g., a home that secures a mortgage. By contrast an unsecured creditor whose debtor cannot pay even after litigation or bankruptcy may get nothing. A smart contract payee can be sure that

[96] This is similar to the example used by Blockgeeks.com to illustrate what a smart contract is. See Blockgeeks.com, A Beginner's Guide to Smart Contracts, available at https://blockgeeks.com/guides/smart-contracts/ (last visited on Oct. 2, 2017).
[97] Stark, *supra* note 94.
[98] See https://www.legalzoom.com (last visited on Oct. 2, 2017).
[99] Stark, *supra* note 94. It is easy to complicate this example to account for interest. With interest at a rate of r per day, the smart contract would simply require B to have $600/(1+r)^2 < 600$ rather than 600 in her account on Sept 29.

her counterparty will not otherwise spend or encumber the money that she expects to be paid under the smart contract. By contrast an ordinary contract payee faces the risk that her counterparty will not have the money to pay her, leaving her with the same recourse as the unsecured creditor. Of course, the ordinary contract payee can try to obtain a security interest, but that just means that smart contracts and security interests are substitutes, underlining our point that the two are roughly analogous.

When combined with an open database of transactions, such as that maintained by a blockchain network, smart contracts can disproportionately reduce counterparty risk in the economy. To illustrate, let us complicate the rental example by allowing that B must earn income each month to pay rent. Specifically, on the 1st of the month B's account, which had $600 falls to $0, but B expects to get a bi-weekly paycheck of $1000 (net of taxes). To address the risk that B's bi-weekly paycheck may not arrive, e.g., because she is demoted or she takes unpaid leave, the smart contact could include an algorithm that predicts income and, on that basis, encumbers the account to protect rent payments. When income is more uncertain, the encumbrance should be larger to ensure a given level of confidence, say 95%, that rent payments would be made on time. Indeed, the rental contract price itself could – and from A's perspective should – be a function of how predictable B's income is. This means that, if B's employer also signed a smart contract, her income would also become more secure and she would have to pay A less for rent! In this manner, the more that smart contracts spread the less uncertainty counterparty risk there is and the less insurance – in the form of higher prices – needs to be purchased against that risk. The money freed up by lower insurance payments could be spent on investment, which should increase growth.

3. Smart contracts reduce uncertainty about interpretation (legal risk)

A second source of risk that smart contracts can address is interpretation risk. When two parties write a traditional contract, there may be ambiguities in meaning. Those ambiguities are subsequently resolved by a court or equivalent adjudicator. But from an ex ante perspective, that resolution is still risky.[100]

We can illustrate with a simple example. Suppose that A and B write a paper contract on Monday that says

> A will supply B a widget on Friday. B will pay $100 upon delivery of the widget. If A does not perform, A owes B $150.

Suppose further that on Tuesday a hurricane strikes, destroying A's factory and inventory, so that he cannot perform on the smart contract. If B sues A in state court for liquidated damages, a court could decide in at least two ways. First, the court could say the contract has an implied force majeure clause, perhaps because that is what the parties would have agreed to if they had considered the possibility of a hurricane white writing their contract, and so A did not breach and owes B nothing. Second, the court could say the four corners of the contract includes no force majeure clause, so A did breach and owes B $150.

[100] See, e.g., Preston M. Torbert, A Study of the Risks of Contract Ambiguity, 2 PKU TRANSNATIONAL LAW REVIEW 1, 5 (2014), available at http://stl.pku.edu.cn/wp-conte`nt/uploads/2014/04/1Torbert_A-Study-of-the-Risks-of-Contract-Ambiguity_20140427.pdf (last visited on Oct. 2, 2017).

When writing the contract, each party formed an expectation about what a court would do, and accounted for that expectation in the price upon which they agreed. If one of the parties was risk averse, the price might have to reflect insurance provided to that party to insure it against the risk from court interpretation (not just the risk of a hurricane). If the parties disagreed on what would happen, they might not agree on a price. If, e.g., A's expectation about the cost of supplying a widget was greater than the B's expectation about the probability of getting the widget times the value of the widget to be, there would be no range for bargaining. In short, if the parties were risk averse or if the parties disagreed about what a court would do, it would be more likely that the parties would not come to an agreement.

A smart contract can reduce the interpretation risk. Because a computer interprets a script like a strictly textualist court would, i.e., it looks only at the four corners of the contract, the outcome may be more predictable than when a court's interpretive methodology is uncertain. In fact, it is possible to do even better than a strictly textualist court because it is possible to cheaply and quickly simulate and thus predict how a computer would execute a smart contract script under a wide array of parameter values for contract inputs.[101]

Anyone who has written code might object that code is very finicky, but this is a negligible cost. For example, a misplaced semi-colon might cause the smart contract to not execute at all. But one can test the contract in a sandbox[102] and see if it executes even before it is actually executed in a live environment.

A potentially stronger objection is that the parties might not intend what the four corners of the smart contract says, but even this is not compelling. The parties can write a different script. Alternatively, default rule code can be written that fills gaps in smart contracts and the parties can reference that default rule code when scripting their contract. In other words, they can't pick the interpretive methodology, but they can pick their default rules.

The magnitude of the benefit from reducing interpretive risk, like the magnitude of the benefit of reducing counterparty risk is uncertain. While the former may be smaller than the latter, it could still be significant. The former may be what drives contractual parties to agree to assign jurisdiction or arbitrate decisions or to move transactions within a firm.[103] Most consumer contracts have arbitration clauses and half of all trade occurs within firms.[104] Reduced interpretive and counterparty risks are not the only reason why the parties may use arbitration clauses or prefer intrafirm transactions, but they are

---

[101] See Blockgeeks.com, A Beginner's Guide to Smart Contracts, *supra* note 96 (citing Bill Marino, Smart Contracts: The Next Big Blockchain Application, Dec. 2, 2015, available at https://tech.cornell.edu/news/smart-contracts-the-next-big-blockchain-application (last visited on Oct. 2, 2017)).

[102] A sandbox is a software developer term for a simulated environment where code can be tested to see if it works or what its impacts might be before it is actually deployed in the real world. See Sandbox (software development), WIKIPEDIA, available at https://en.wikipedia.org/wiki/Sandbox_(software_development) (last visited on Oct. 2, 2017).

[103] Michael Gruson, Governing Law Clauses in Commercial Agreements—New York's Approach, 18 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 323 (1980).

[104] See Jay Tidmarsh, Out of Court, Out of Luck, USNWR (March 19, 2015), available at https://www.usnews.com/opinion/economic-intelligence/2015/03/19/consumer-protection-bureau-arbitration-report-provides-much-needed-data; Pol Antràs, Firms, Contracts, and Trade Structure, 118 QUARTERLY JOURNAL OF ECONOMICS 1375 (2003).

significant risks. Indeed, counterparty risk is what spawned the creation of blockchain in the first place.[105]

V. HOW SMART CONTRACTS ON BLOCKCHAIN CAN HELP REDUCE CONTRACTUAL HOLDUP

Our central claim is that smart contracts on blockchain networks allows parties to more credibly commit to original contracts (in case they want to prevent any renegotiation) or to mechanisms to structure renegotiation or make information verifiable to courts (in case they want specifically to stop hold-up). Here we explain how practically to do that. The implementation we suggest requires some assumptions and we will clarify those as well.

A. An example with the ADR renegotiation design mechanism

Suppose that Apple and Corning wish to write a contract that includes an ADR mechanism to structure renegotiation after a holdup so that the holdup does not deter efficient relationship specific investment. Recall that the ADR mechanism requires one party be given a default option and the other the credibility to make a take-it-or-leave-it offer. Each requires commitment, i.e., the latter party must have strong incentives not to a second offer and the former a strong incentive not to renegotiate the default offer. How could the parties implement this with these new technologies?

Learning from Section III.D.1, we would first ask how much information the parties have. If it is enough to devise a renegotiation design or revelation mechanism, then the parties would want to construct a penalty provision that deters deviation from the mechanism and that cannot be undone by courts or the parties through renegotiation. If the amount of information is not adequate to devise such mechanisms, the only thing the parties can do is construct a penalty provision that discourages any deviation from the original contract. Of course, such a penalty provision would also bar renegotiation due honestly to changed circumstances and that does not affect ex ante incentives to invest. So the parties should not construct a penalty that locks in the original contract unless the expected cost of holdup is greater than the expected cost of inflexibility.

To illustrate how a penalty clause could be constructed, suppose the parties have enough information to write an ADR renegotiation design mechanism. Let's see how the penalty provision would work. First, we examine the default option. In our example, it is Corning that is to be given the option to trade a unit with probability 5/6 at price 23 1/3. We would script a clause in the smart contract code that says Corning can ask for the default trade and if that trade is not consummated, then Apple pays a penalty. Likewise, the smart contract code would make Apple pay a penalty if it communicated a second offer to Corning after Corning refused its first ostensibly take-it-or-leave-it offer.

In order not to skew the incentives of the parties when playing the ADR game, the penalty must flow to a third party.[106] For instance, if the smart contract does not observe the default trade by a certain time

[105] Bitcoin, the first application of blockchain, was created to solve the double spending problem. See Nakamoto, *supra* note 67, at 1.
[106] See text accompanying *supra* note 62.

or if it observes a second offer from Apple, then the code would irreversibly transfer money from Apple to anonymous third parties.

Blockchain makes it possible for penalties to flow to third parties. All the smart contract has to do is specify that some large amount would be transferred from Apple's account (its public address or key) on the network to a randomly generated list of public addresses or keys and that the smart contract would announce to the blockchain network the private keys associated with those public keys. The latter step would allow any node on the network to access and transfer to their account the money at those public addresses. It would as if the code announced that there was a pile of cash on the corner of Broadway and Fifth Avenue in Manhattan: people would rush to take the money.[107] The entities that collect the money distributed by the smart contract would be able to remain anonymous – as blockchain allows anonymous transactions.[108] If that entity were located in a country that did not have a know-your-customer (KYC) requirement, they could also convert that money into the government currency of their choice. There are plenty of countries happy to do that.[109]

The penalized party, and perhaps even the non-penalized party, would have an incentive to go to court to enjoin the penalty. With the default option, Apple would have an incentive to not be penalized for defying Corning's request. With Apple's take-it-or-leave-it offer, Apple has an ex post incentive to avoid the penalty for making a second offer and Corning has an incentive to receive a second Apple offer, meaning both would want to petition a court.

The future commitment feature of smart contracts and the irreversibility of blockchain transactions can render court injunctions ineffective. Once the parties sign the agreement, future exchanges are already booked and cannot be undone – by either the parties or a court – without having either a majority of the computing power or the tokens on the blockchain.[110] A court does not have that. Thus, a court can no more require a transaction on blockchain be reversed than it can require that the stock price of a company that committed fraud increase to compensate shareholders.

Court-ordered damages would not help undermine the smart contract commitment. For one thing, punishing Corning because Apple has to pay a penalty does not change Apple's incentives unless Corning has to pay Apple to compensate for the penalty Apple must pay. But if Corning has to pay Apple, then the penalty script in the smart contract can make the penalty contingent on subsequent damages ordered by a court. For example, if the optimal penalty on Apple for say, making more than one offer, is 100 and the damages awarded by the court for making Apple pay a penalty is D, the script could say Apple must pay 100 + D.

---

[107] Antonopolous, *supra* note 72, at 17 (explaining how transferring money to a public key for which the private key is publicly known would lead to loss of funds).

[108] See Ikye Aru, Blockchain Transaction Anonymity is Necessary Evil, COINTELEGRAPH (Apr. 18, 2017), available at https://cointelegraph.com/news/blockchain-transaction-anonymity-is-necessary-evil (last visited on Oct. 2, 2017).

[109] See, e.g., U.S. Department of State, Major Money Laundering Countries (Mar. 7, 2012), available at https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184112.htm (last visited on Oct. 2, 2017); IRS, List of Approved KYC Rules, available at https://www.irs.gov/businesses/international-businesses/list-of-approved-kyc-rules (last visited on Oct. 2, 2017); and PWC, Know Your Customer: Quick Reference Guide (Jan. 2013), available at https://www.pwc.com/gx/en/financial-services/assets/pwc-kyc-anti-money-laundering-guide-2013.pdf (last visited on Oct. 2, 2017).

[110] See Section IV.A.3.

Apple may be tempted to hold Corning up but avoid penalties by renegotiating in two steps. First, they would comply with the ADR mechanism in the original contract. Second, they would simultaneously write a separate contract with Corning that functionally puts Apple in the same position as if it had successfully help up Corning in the original contracts. This second contract would say that Corning will sell to Apple one unit of Gorilla glass at a price that is equal to the price the parties would negotiate for Gorilla glass in the abstract (say p_2) minus an amount equal how much a successful hold-up in the original contract would benefit Apple. This benefit is equal to the difference between the price that the original contract specified (p_1) and the price Apple could extract if it were able successfully to hold Corning up ($p_H < p_1$). In short, the second contract price would be $p_2 - (p_1 - p_H)$.

Blockchain can be used to prevent renegotiating through subsequent contracts as well. The smart contract could crudely specify that, if there were a second exchange between Apple and Corning, the penalty would be triggered. Of course, that approach would have collateral damage: the parties may reasonably want to trade a second time and this penalty trigger would prevent that. To address that, the parties could agree that the penalty would only be triggered if the second contract had a lower price than the first contract, though this would create problems if Corning's costs fell over time. Alternatively, they could even configure the smart contract to both structure renegotiation on the first trade and to provide a framework for subsequent trades.[111] That framework includes a revelation mechanism for subsequent trades that would allow the smart contract to compare the price and cost c of the subsequent trades to ensure that Corning was fully reimbursed for its investment in prior to the first trade.

A natural question is how the smart contract code would know if Corning or Apple violated the default option or final offer or negotiated a subsequent contract that de facto renegotiated their original contract. The smart contract can certainly monitor the blockchain – the ledger of transactions – on the network, in which case it would know directly if another trade occurs. It is here that the open feature of blockchain is critical. It could also monitor communications or accounts not on the blockchain network by using application program interfaces (APIs) that gave it access to the parties' messages or to other accounts the parties may have.[112] When the parties sign the contract, they want the penalties so they would have an incentive to allow the smart contract access to all their messages and accounts.[113]

Of course, the fact that the parties want to share information does not mean it is easy to do so. It may be difficult to give access to all communications between parties, e.g., in person conversations between

[111] This is not uncommon in long term contract where the end date is not specified. See, e.g., Susana López-Bayón & Manuel González-Díaz, Indefinite contract duration: Evidence from electronics subcontracting, 30 INTERNATIONAL REVIEW OF LAW AND ECONOMICS (2010).

[112] See https://plaid.com/ for an example of how this might work. For more information on other similar services, see this thread on stack overflow: https://stackoverflow.com/questions/7269668/is-there-an-api-to-get-bank-transaction-and-bank-balance (last visited on Oct. 2, 2017) (noting that Yodlee.com and Mint.com do the same, though banks may charge a few to access the API).

[113] If one of the parties did not, then the other party would not want to enter the contract with that party. As a result, the party that considered not giving access would give access because ex ante they would benefit from the contract, even at the cost of giving access. Especially since access to the smart contract is not the same as public access, as the smart contract would not share the messages or account information with anyone, even counterparties.

employees of the two parties.[114] It may also be that the parties have accounts at some banks that do not provide APIs that can give the smart contract access and the parties cannot change those banks' policies. We hope this is a limitation that recedes in time as more accounts become interoperable in the sense of providing API access. We also think it may not be a large limitation as parties certainly have an incentive to keep most of their money in accounts with banks that offer APIs as those APIs allow the parties themselves to monitor their own accounts more easily.

B. Generalizing the example

Having shown through example how ADR provisions might be implemented, we can infer how the provisions required for a revelation mechanism or the original contract as a whole can be implemented via smart contract. The smart contract can employ penalties to get the parties to comply with specific steps of the revelation mechanism. To complete each mechanism, the smart contracts must require that parties take actions in a certain sequence, e.g., the take-it-or-leave-it offer comes before the default option can be triggered, otherwise the party that was not supposed to move faces penalties. Since the renegotiation-design mechanism is the whole contract, the parties that want to employ that mechanism need only specify the steps that mechanism requires. Parties that wish to employ the revelation mechanism can only finalize their smart contract by adding to their revelation mechanism a schedule of contingent trades that are each triggered by different combination of valuations v and costs c revealed through the revelation mechanism.

For those parties that do not have the relevant information to devise renegotiation design or revelation mechanisms, blockchain still has value. Such parties have to make a choice: write a contract that never allows renegotiation, or always allows renegotiation, whether due to hold-up or to changed circumstances. If they think the hold-up problem is bigger than the problem of inflexibility, they can bar renegotiation under any circumstance by imposing penalties for such renegotiation. The steps were outlined above.

C. Robustness of smart contracts on the blockchain

Smart contracts on the blockchain have at least three limitations we have not yet discussed. One is that government may simply ban blockchain or smart contracts that impose penalties.[115] We do not think this is likely. Blockchain has a great deal of value outside the contractual commitment setting. Entities

[114] Various email providers, e.g., Google, allow API access to email, but typically only for the owner of the account, not third parties, including smart contracts. For google see https://developers.google.com/gmail/api/ (last visited on Oct. 2, 2017); more general see also https://context.io/. However, if there is demand for this, there is no technical barrier to it. In any case, the account owner can provide the smart contract script this power. This is no different than an IFTTT (acronym for if this then that) script that signals to third parties the actions of an account owner. For IFTTT examples with Gmail as an input, see https://ifttt.com/gmail.

[115] See, e.g., Timothy B. Lee, It looks like China is shutting down its blockchain economy, ARSTECHNICA (Sept. 15, 2017), available at https://arstechnica.com/tech-policy/2017/09/china-may-be-getting-ready-to-ban-bitcoin/ (last visited on Oct. 2, 2017) (noting that China has shut down cryptocurrency exchanges). However, this does not mean all blockchain networks are banned in China.

that obtain that value would lobby or litigate hard against a broad ban of blockchain.[116] A narrower ban on smart contracts with penalties is more plausible. It would be akin to a ban on penalty clauses.[117] The main problem is that the ban is difficult to enforce. Both parties to a contract with a penalty want that penalty ex ante, so have little incentive to report that they have written a smart contract with a penalty. And ex post a court cannot rescue them from that penalty, if the penalty is written correctly.

Only a whistleblower, a third party, or a contractual party who was coerced into agreeing to a smart contract penalty clause has an incentive to get courts involved. But legislators would have to authorize bounties for whistleblowers, another type of third party standing, or criminal penalties. Those may be political hard sells because no outsiders are hurt by the commitment described in this paper. The biggest risk comes from coerced parties. Indeed, it is likely these individuals who were able to undermine penalty clauses in non-smart contracts. Perhaps the difficulty of enforcing a ban on all smart contracts with penalty causes will give courts an opportunity to limit their ban such agreements to those where one of the parties is unsophisticated and may have been coerced into signing it.

A second limitation concern with smart contracts on blockchain is that, like computer scripts generally, they are sensitive to honest mistakes. For example, if Apple accidentally hits send on its email that contains a draft – but not the final draft – of its take-it-or-leave-it offer, the smart contract will not allow it to recall the message otherwise Apple could circumvent the smart contract by calling its first offer a message it wants to recall. To address the costs of such mistakes, game theorists sometimes look for equilibria of games that are robust to "trembling hands"; correlatively mechanism designers might look for game rules that yield trembling hand perfect or robust equilibria.[118] We do not know if the mechanisms we have discussed in this paper are robust to errors, though empirical work by Aghion et al. (2017)[119] give us some hope that smaller mistakes might yield smaller deviations from first best incentives to invest.

A third limitation of the smart contract penalties is that they only work if the parties have sufficient assets to pay the penalties required by the smart contract. One way to ensure that smart contract penalties can be implemented and are effective is for the parties to place enough assets in their accounts on the blockchain network to cover penalties until both parties satisfactorily perform on the contract. Note that these assets are available to be employed or spent until penalties are required if the parties take out a loan collateralized by the assets in their account on the blockchain. Another way to ensure penalties can be covered is to not require the parties to put up a bond on the blockchain but to allow the smart contract to create debt on behalf of the penalized party to a lender, with the proceeds from the lender being used to pay third parties pursuant to the penalty. The lender would be willing to do so long as the party on the hook for the penalty had enough assets, on the blockchain or otherwise. Of course, if either party did not have enough assets to cover optimal penalties, optimal penalties would

[116] See Jon Matonis, Government Ban On Bitcoin Would Fail Miserably, FORBES (Jan. 28, 2013), available at https://www.forbes.com/sites/jonmatonis/2013/01/28/government-ban-on-bitcoin-would-fail-miserably/#5d5e61c61d25 (last visited on Oct. 2, 2017).
[117] See Farnsworth, *supra* note 21, at 845.
[118] R. Selten, Reexamination of the perfectness concept for equilibrium points in extensive games, 4 INTERNATIONAL JOURNAL OF GAME THEORY 25, 38 (1975).
[119] See Aghion et al., *supra* note 49, at 27.

not be available. In that case penalties would have to be lowered, and hold-up risks would rise commensurately.

CONCLUSION

In this paper, we have highlighted the problem of holdup, a specific type of transaction cost that can reduce parties' incentives to make relationship-specific investments or to trade in the first place. We argued that traditional contracts, made on paper and enforced with existing financial technology and litigation strategies, cannot provide the very high level of commitment necessary to limit the harms from holdup. Finally, we explained that smart contracts on blockchain networks have features that, when these technologies become widely deployed, may be able to provide a greater degree of commitment and thus additional protection against holdup.

We conclude by considering the implications of our argument for the size of firms, and offer some thoughts about the benefits of smart contracts and blockchain for contract law more generally.

A. Implications for size of firms

One implication of our claim is that blockchain and smart contracts have to the potential to increase the gains from, and thus amount of, relationship-specific investment and trade and thus total output that we observe in the economy.[120] The degree of benefit is proportional to the extent to which holdup is a drag on investment and trade. In addition, we expect that blockchain should reduce the size of firms. As blockchain increases the returns to market-mediated transactions, firms will move more transactions outside the firm to the market. In this way, it functions much like prior technological innovations that increased counterparty trust and accountability.[121] Blockchain may also do this by reducing the role of trust intermediaries, such as banks, in the economy, though that is not a feature we emphasize in this paper.[122]

B. Speculation about effects on contracting generally

While our focus has been smart contracts on the blockchain can tackle the problem of holdup in contracts, there may be other benefits of these technologies to contract law generally. One that we think particularly important is that they may reduce the need for centralized entities, especially courts, to resolve contractual disputes. We think this is possible through at least two channels. First, as we explained in Section V, smart contracts can reduce the need for court interpretation of contracts. A smart contract script, like other computer code, does what it does. The language compiler is the

[120] Oliver E. Williamson, Transaction-Cost Economics: The Governance of Contractual Relations, 22 THE JOURNAL OF LAW & ECONOMICS 233 (1979).
[121] More generally, see R.H. Coase, The nature of the firm, 4 ECONOMICA 386, 388 (1937). For an example of how technology can have this effect, see George P. Baker & Thomas N. Hubbard, Contractibility and Asset Ownership: On-Board Computers and Governance in U. S. Trucking, 119 THE QUARTERLY JOURNAL OF ECONOMICS 1443 (2004).
[122] Antonopolous, *supra* note 72, at 4.

interpreter and it does not permit variation in interpretation. Parties can tackle bugs in the code via simulation, but they get what the code does. In some sense, the compiler is the ultimate textualist interpreter, with little regard for absurdities. Parties do not have to use it, but they have the option to. When they do, the role of courts will decline to a greater or lesser extent.

Second, blockchain networks may use their validation mechanism or their consensus rules to adjudicate smart contract disputes. If a smart contract crashes because it is poorly written or if a party feels the counterparty somehow did not honor a smart contract,[123] the network can appoint a third party node on the network not just to witness the contract, but to adjudicate the dispute. The idea would be that, just as the Bitcoin network replaced banks as the intermediary for payments, it can replace courts as arbiters of smart contract disputes.

Of course, the difficulty is that the work required to adjudicate smart contract disputes may not be as algorithmic as mediating transactions. The latter require only that the third party verify the sender of money has enough money in its account (which is evident from the blockchain ledger up until the date of payment) and that the transfer to the receiver's account is recorded in the updated blockchain ledge. Resolving contract disputes requires, for example, determining what the parties would have scripted if they had considered the state in which the smart contract crashed. This requires fact finding beyond the information already available on the blockchain.

It is not clear that other nodes, or even a consensus among nodes, is a good way to resolve the problems. The cost of fact finding of the sort required for adjudication is greater than the cost of fact finding required to verify a payment. The third-party node has to be compensated for that higher cost, just as it is compensated for verifying transactions. Moreover, the other nodes may not be well qualified to adjudicate disputes. The idea of using blockchain is not entirely ludicrous, however. Civil trials, including contract trials, in existing courts also impose great costs on parties. Moreover, the may be tried to a jury, which also may not be qualified.

Even if a blockchain-mediated peer-to-peer network does not displace courts, it may be able to complement courts in two ways. First, it may help courts better identify majoritarian default rules. The more smart contracts are written on the blockchain, the easier it would be for courts to determine true majoritarian default rules. This is difficult now as selection into litigation determines what judges see[124] and general fact finding is limited or biased by the adversarial process.[125] As a result, there are reason to suspect that courts may not be filling in gaps in contracts with the right default rule. But because contracts on the blockchain may be public, the court can directly query what most parties want in specific situations.[126]

Second, just as parties now can set the jurisdiction that will govern their contract disputes, smart contracts may even allow parties to specify which set of (scripted) default rules should govern the gaps in their contracts. This process would be similar to the way in which people putting up intellectual

[123] E.g., perhaps the counterparty negotiated around it off the blockchain.

[124] See, e.g., Scott Baker & Anup Malani, Trial Court Budgets, the Enforcer's Dilemma, and the Rule of Law, 2014 U. ILL. L. REV. 1573, 1577 (2014).

[125] See, e.g., Christopher Tarver Robertson, Blind expertise, 85 NYU L. REV. 174, 177 (2010).

[126] This is not actually perfect because, even if everyone makes their contracts public, there may be selection into who actually writes provisions that covers specific circumstances. However, it is true that blockchain reduces one layer of selection – namely selection into litigation.

property (IP) such as photos or images onto web might simply appeal to the Creative Common license to govern the usage of their IP. This would lower the demand for courts, but in case disputes go to trial, it would help courts decide cases.

C. The importance of blockchain and smart contracts

With many new technologies that come along, there are a wave of articles that claim the technology fundamentally changes law. They risk creating what Judge Easterbrook called the law of the horse.[127] We do not yet think that blockchain and smart contracts will change contract law. Rather, we think it may have a measurable impact on the sorts and amounts of contracts that can be written. To justify our beliefs, we need only to point to the substantial amount of investment going into blockchain. A large fraction of the largest banks, IT companies, and consulting firms are investing in blockchain.[128] The total number and value of transactions on the Bitcoin and Ethereum networks, while still far short of even Paypal, are growing rapidly.[129] Finally, the total amount of money raised through Initial Coin Offerings (ICOs) exceeded the total amount of venture funding in the last quarter.[130] While we do not think there is enough data to conclude that blockchain will change the world, let alone law, we do think there is enough activity in the technology to begin considering the legal implications of this technology, including, as we do in this article, how blockchain and smart contracts affect contracting.

[127] Frank H. Easterbrook, Cyberspace and the Law of the Horse, U. CHI. LEGAL F. 207 (1996).

[128] This includes Bank of America Merrill Lynch, Wells Fargo, Citigroup, TD Bank, BBVA, Bank of New York Mellon, Northern Trust, HSBC, Barclays, UBS, Intel and Temasek, which are part of the R3 consortium (see Penny Crossman, Banks pour $107M into blockchain consortium R3, American Banker (May 23, 2017), available at https://www.americanbanker.com/news/banks-pour-107m-into-blockchain-consortium-r3 (last visited on Oct. 2, 2017)); Accenture, American Express, Cisco, Diamler, Fujitsu, IBM, NEC, and SAP in the Hyperledger consortium (see https://www.hyperledger.org/members); and BBVA, BP, Deloitte, ING, Infosys, J.P. Morgan, Mastercard, Microsoft, Samsung, Santander, Scotiabank, Thomson Reuters and UBS that are part of the Enterprise Ethereum Alliance (see https://entethalliance.org/members/).

[129] See Bitcoin and Ethereum vs Visa and PayPal – Transactions per second, Altcointoday.com (April 22, 2017), available at: http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/ (last visited on October 2, 2017); Bitcoin, Ethereum, Litecoin, Dogecoin Transactions historical chart, Bitinfocharts.com, available at: https://bitinfocharts.com/comparison/transactions-btc-eth-ltc-doge.html (last visited on December 27, 2017).

[130] Arjun Kharpal, Initial coin offerings have raised $1.2 billion and now surpass early stage VC funding, CNBC (Aug. 9, 2017), available at https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html (last visited on Oct. 2, 2017).

APPENDIX I: ADDRESSING HOLD-UP WITH OPTIONS CONTRACTS (NOLDEKE AND SCHMIDT 1995)

Noldeke and Schmidt (1995) show that certain option contracts can also achieve the social optimum.[131] Their reasoning is as follows.[132]

The first step is for the buyer and seller to design the renegotiation bargaining game. Here, Noldecke and Schmidt (1995) adopt the following formulation that was first contained in Hart and Moore (1988).[133]

After v and c have been realized, suppose the buyer and seller can simultaneously send each other new offers. Each offer (from each party) is a pair of prices: one if there is trade and one if there is no trade. Trade is assumed to be verifiable by a third party such as a court, and thus the specified payment can be enforced. Said payment is the default, unless one of the parties decides to furnish the court with the new offer from the other party. In equilibrium only two offers will be furnished: (i) the seller accepting a higher price; or (ii) the buyer accepting a lower price.

Now, suppose the seller receives some default payment d if no trade occurs, but has the option to deliver the good to the buyer and receive an additional payment p, so that the total transfer $t = d + p$. The question is how renegotiation works. There are three different cases to consider.

First, suppose that p is less that "low c". If there is no renegotiation the clearly the seller does not want to trade because no matter what her production cost is she will receive less than that amount from the buyer. But if the buyer's valuation is high and the seller's cost is low then there are gains from trade, and thus renegotiation should occur. Raising p to "low c" will be sufficient to do this, and the buyer does not need to go any higher. To see this, note that if the buyer furnishes a letter offering $d +$ "$low\ c$", the seller will want to trade. Moreover, the buyer knows that the seller will want to deliver the letter to the third party/court. Since p is equal to "low c", the buyer extracts all the surplus, which is equivalent to saying that she has all the bargaining power.

Second, suppose that p is between "low c" and "high c". As before, the buyer can extract all the surplus from renegotiation by sending furnishing a letter agreeing to a higher price if there is no trade.

Third, suppose that p is greater than "high c". Now the seller always wants to trade. Again, the buyer can extract all the surplus from renegotiation by sending furnishing a letter agreeing to a higher price if there is no trade.

Taken together this means that the buyer has all the bargaining power and therefore has appropriate incentives to make the optimal level of investment.

[131] Noldeke and Schmidt, *supra* note 20, at 168-171.
[132] We follow Bolton and Dewatripont, *supra* note 5, at chapter 12, closely here.
[133] Noldeke and Schmidt, *supra* note 20, at 165.

APPENDIX II: FACTORS THAT AFFECT THE VALUE OF BLOCKCHAIN AS A WITNESS TO STATEMENTS

Knowing that blockchain is analogous to having a witness publicly validate statements, we can determine when blockchain is valuable and when it is not. These in in turn can help explain when it is and is not a valuable solution to business problems and some of the specific technical details about the structure of blockchain networks.

A. The parties to a transaction should be speaking the truth

Having a witness, and thus blockchain, is valuable when A and B make statements that are contrary to their interest or that they have an incentive to make only if they are truthful. For example, A says he is going to give B an apartment and B says she is going to give A $600/month. In this case the witness to the statements against interest allows her to credibly say B has a right to the apartment and A has a right to $600/month (and equivalently that A no longer has occupancy rights to the apartment and that B is $600/moth less rich.) If instead A said C owes B $100, then the witness would not allow B to claim she is $100 richer, as C was not part of initial statement.

B. The witness must be objective

The witness must be a neutral observer. Blockchain is valuable when the nodes that validate transactions are not involved in, and do not benefit from, the transaction. Thus, A's friend C cannot be a witness to a statement from B that B is going to pay A $600/month. More brashly, A's friend C cannot add a hash to the blockchain that says B will pay A $600/month even if B did not say that. To keep such things from happening, the network does two things. First, it assigns the task of validation either by having a competition to see who is the first to validate an announced transaction (so-called "proof-of-work" validation), or by having people vote on what the announced transaction is (so-called "proof-of-stake" validation). Second, it requires the witness to have a special code[134] that proves that B actually said what the witness heard.

C. The witness must have an incentive to do her job

The witness must be given adequate incentive to attest to statements. On the Bitcoin blockchain network, for example, the nodes that witness or validate messages from A and B are called "miners". The Bitcoin network uses "proof-of-work" validation, meaning miners compete to be the first to validate that A and B announced a transaction. Whichever miner wins the competition is given two payments. One payment comes from the network: the network issues a token called Bitcoin to the winning miner. The other payment is a small commission, again in the form of tokens, from A and B. These tokens – called Bitcoins on the Bitcoin network – are valuable because people are willing to trade Bitcoins for

[134] Specifically, the witness C must have a code that is called B's "public key." That code too is the output of one-way function, again a hashing function, the input to which is a secret code that only B knows and that is called B's private key. If C announces the public key, then it only unlocks B's account if the private key that maps to the public key is B's private key. The address will map only if B intended the transaction. Only if B intended the transaction will she provide a public key to C that is actually the hash of her private key.

widely used fiat currencies such as the U.S. dollar and the Euro. Other networks give out other tokens for nodes that validate the announcement of transactions. The value of the incentive is a function of how much people are willing to pay for the tokens, as that determines the real-world consumption the tokens afford the witnesses.

Making tokens valuable is a separate problem that each different blockchain network must solve. The Bitcoin network solved the problem by promoting Bitcoin tokens (called simply Bitcoins) as a form of currency, allowing people to pay each other with tokens. If one can buy a coffee for 1 Bitcoin and a coffee costs $2.50, then 1 Bitcoin is worth $2.50. Ethereum promotes its tokens, called Ether, because they can be used in a wider array of transactions, not just payments but also execution of smart contracts. The more people that use a network for obtaining services (other than witnessing), the more valuable will be the tokens that are used as currency on that network.

In many cases, the act of witnessing – specifically publicly witnessing – a transaction has not just private benefits to the transacting parties A and B, but also public benefits to third parties, such as those who might transact with A and B in the future. In this context, the amount that A and B alone would pay for the witnessing function may not be enough to ensure all socially valuable witnessing takes place. This is an important risk to any proposal to have just commissions from A and B compensate nodes for validating a transaction, as the Bitcoin network proposes to do at some point in the future.[135]

In addition, since information is a public good, the public announcement of the witness creates a collective action problem. A common solution is a tax, in this case on all possible parties that might transact with A and B to pay for the witnessing costs, especially when they exceed the commissions A and B are willing to pay. Economies of scale in public goods and the possibility of future transactions with A and B on other platforms may be what leads to centralized ledgers or registries, typically in the hands of the government.

D. Blockchain witness technology has to be competitive with existing witnessing technology

The process of witnessing that blockchain sets up must either be more credible than the old fashioned approaches to witnessing or less costly than those methods or both, otherwise there is no reason to use blockchain. The original application of blockchain, the Bitcoin network, was as a method of making payments, i.e., B saying she is going to pay A $600. It was not a method of contracts. It was advertised as a cheaper method of making payments than, say, ACH or debit cards, which charge $0.56 per transaction and 1.5-2.5% of transaction amounts, respectively.[136] The cost of making a payment with Bitcoins was at least the value of the tokens given to miners for validating announced transactions.[137]

[135] The Bitcoin network has announced it will issue just 21 million tokens, after which the only payments to witnesses would be commissions paid by transacting parties, i.e., A and B in our example.

[136] Association of Finance Professionals, Payments Cost Benchmarking Survey: Report of Survey Results 8, 16 (2015)

[137] It was not just the value of the commission paid by A and B to the miner who was chosen to be the witness because each miner competing to be a witness for A and B would expend as much energy on the competition as the payoff to being selected a witness times the probability of being selected. The payoff to being selected is the commission plus the new Bitcoins the network issued to each winning miner. Summing up across all the miners competing, the probabilities of winning have to be one. Indeed, the economic literature on patent races suggest that the total energy spent could actually be more than the total payments to miners. See Loury (1979).

As the price of Bitcoin rises, the cost of validation increases. If the amount of energy spent by all miners to validate transactions is smaller than the cost of validating the same transactions via the traditional technology, the Blockchain has value as a witnessing technology.