The Georgetown Law Technology Review

Articles

The Law and Legality of Smart Contracts

Max Raskin

April 2017

Cite as: 1 GEO. L. TECH. REV. 304 (2017)

Perma: https://perma.cc/UC8L-KTW3

(Download PDF)

A new technology called "smart contracts" has emerged. What makes these legal agreements innovative is that their execution is made automatic through the use of computers. This Article examines smart contracts from a legal perspective. Specifically, this Article explains smart contracts' operation and place in existing contract law. It introduces a distinction between strong and weak smart contracts, as defined by the costs of their revocation and modification. The article concludes that smart contracts are simply a new form of preemptive self-help that should not be discouraged by the legislatures or courts. While certain unconscionable examples of strong smart contracts may need to be policed, judges and policymakers should foster a climate that treats smart contracts as another form of more traditional agreements.

Introduction

Self-help is nothing new. Whether building walls to stymie trespassers or changing locks to evict squatters, individuals regularly act on their own before invoking the formal legal system. Over the past few years, a group of innovators have begun designing computer technologies that bring self-help to the realm of contracts.[1] They call these new contracts "smart contracts." Their aim is to allow contracting parties to ensure their agreement is enforced by raising the costs of any breach by a prohibitive amount.

Smart contracts are defined as agreements wherein execution is automated, usually by computers. Such contracts are designed to ensure performance without recourse to the courts. Automation ensures performance, for better or worse, by excising human discretion from contract execution.

One example of a smart contract is the humble vending machine. If the machine is operating properly and money is inserted into the machine, then a contract for sale will be executed automatically. This is a smart contract. Such a contract poses no legal problems if the machine were to dispense soda, but legal questions arise if the machine instead dispenses heroin. Should laws be passed to ban vending machines because they can be used to further illegal ends? Or should their use be regulated ex post?

Certain situations will arise that will force the law to deal with smart contracts, and the purpose of this article is to assess their legality and demonstrate that there is little difficulty situating smart contracts within existing contract law. Innovative technology does not necessitate innovative jurisprudence, and traditional legal analysis can help craft simple rules as a framework for this complex phenomenon.[2]

The Article begins with a definition of smart contracts and an explanation of the interplay between legal prose and machines. This analysis will also engage with the existing smart contract research, which is often written from a computer science perspective. The salient features of smart contracts differ between the technical and legal discussions, a fact which is lost in the existing literature. To help clarify, the article will introduce a classification of strong and weak smart contracts. To provide context to the above discussion, a short history of the idea will be included.

Next, the two technological components that have enabled smart contracts will be explained. The first component will be termed "contractware," which can be defined as the physical or digital instantiations of contract terms onto machines or other property involved in the performance of the contract.[3] [4] By instantiation, we mean taking the terms of the agreement and either writing them into previously existing software or writing them into software that is connected in some way to a machine that implements the contract. Take, for example, the innards of our aforementioned vending machine. A physical device within the machine is encoded with a seller's offer. The machine will only dispense a soda if the terms of the agreement are met, for instance, by depositing a Krugerrand into the device. In addition to discussing the legal theory behind the vending machine, the contraption's radical history will also be discussed to remedy the paucity of vending machine literature that exists in legal academia.[5] This history sheds light on the power of the smart contract to protect individual autonomy over state diktat.

There is a second technological component this article will discuss: decentralized ledgers, also known as blockchains. These are databases of information that are created by a network with no central authority.[6] For instance, instead of a public recordation system that exists on paper files stored in city hall, a blockchain system would keep a decentralized ledger on the computers of every node running the software.[7] It has become easier to build and enforce secure contracts without recourse to the state through the use of shared, instead of centralized, consensus-establishing mechanisms. The combination of these components—contractware and blockchains—has made smart contracts that are enforced by a decentralized, third-party network possible.[8]

Part *TK* of the Article will analyze smart contracts through the lens of existing doctrines in contract law. The section will provide an overview of the classic stages of contract formation and pose a series of observations and questions that are implicated by smart contracts. In particular, this section will discuss consideration, formation, avoidance, performance, breach, and remedy. Section TK will explore one existing application of smart contracts: automobile starter interrupters. These are devices that are installed in cars by creditors, allowing them to remotely disable the car if a debtor has breached the terms of an agreement. The subject of this section will be how courts and legislatures have dealt with these devices. This is a current instance where courts have passed judgment on the legality of smart contracts, albeit not self-consciously. They were not setting out to rule on legality, but implicitly did so as a collateral matter.

Next, the Article will examine the benefits of smart contracts. Like many technologies, the creators and early adopters of smart contracts are ideologically driven and believe that the invention can radically alter the nature of society and its relationship with the traditional centralized state. Many believe that private enforcement of contracts can reduce the need and extent of monopolized police and legal services provided by the state.[9] However, the vision of the first movers often gives way to the realities of a conservative world that looks askance at new technologies. There are, however, benefits of smart contracts that do not upend the existing social order, but instead decrease transaction costs by cutting out intermediaries. This allows for industrial society to operate more effectively. These benefits extend to financial transactions, corporate governance, financial products, and a host of other potential applications that have been analyzed by economists.

The final section of the Article discusses both a philosophical and practical set of problems with smart contracts. The benefits of smart contracts must be viewed in light of their inherent limitations. A smart contract asks its parties to tie themselves to the mast like Ulysses and ex ante commit to abiding by the terms of the agreement.[10] In certain instances, the state may want to prevent individuals from committing themselves if the terms of the contract are substantively unconscionable.

Smart Contracts: Strong and Weak

Definition

A smart contract is an agreement whose execution is automated.[11] This automatic execution is often effected through a computer running code that has translated legal prose into an executable program.[12] This program has control over the physical or digital objects needed to effect execution. Examples are a car that has a program installed to prevent ignition if the terms of a debt contract are not met or banking software that automatically transfers money if certain conditions are met. A smart contract does not rely on the state for enforcement, but is a way for contracting parties to ensure performance.

For legal purposes, I will further differentiate between strong and weak smart contracts. Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This means that if a court is able to alter a contract after it has been executed with relative ease, then it will be defined as a weak smart contract. If there is some large cost to altering the contract in a way that it would not make sense for a court to do so, then the contract will be defined as strong.

Numerous alternative definitions of smart contracts have been proposed.[13] In a paper outlining a template for creating standard smart contracts, Clack et al. proposed a broader definition of smart contracts that bifurcates into what they call traditional and non-traditional methods of enforcement.[14] Clack et al. define traditional means of enforcement as those through institutions like arbitration or courts of law – these are weak smart contracts in our classification scheme, because the costs to change or revoke the contract are not high enough to proscribe courts or arbitrators from doing so.[15] They define non-traditional means of enforcement as those through "tamper-proof" technology "with the assumption that in a perfect implementation of the system wrong-performance or non-performance become impossible."[16] This narrower set of smart contracts is what I deem the strong variety. The reason is that the execution of the contract can be "tampered" with by the courts in the sense that the court can alter the original intentions of the parties.

From the perspective of innovators, this bifurcation makes sense because as a practical matter, technology and society are far away from the pure, strong smart contract definition this paper considers. For instance, personal service contracts are not subject to computer control.

Clack et al.'s broad definition does not capture what is unique about smart contracts from a legal perspective. The broad definition that includes instances where courts can interpret and enforce the contract is indistinguishable from a traditional contract law. If a court has power to interpret and then enforce a contract, then it is the smart actor and will abide by previous precedential rules and statutory frameworks. Traditional enforcers who are confronted with contracts that use technology, but ultimately rely on some form of alterable behavior, will be able to award damages, issue injunctions, or enforce criminal penalties to enforce their understanding of the law. For instance, consider a smart contract that requires a party to mow a lawn if funds are dispersed. And suppose the mechanism for enforcing the dispersal of funds was a sensor that measures the lawn's average grass length. Although one side of the contract could be automatically enforced, because the behavior of the human party is alterable by a court, i.e. a court can excuse performance, the contract will not necessarily execute.

But traditional enforcers who are confronted with strong smart contracts will be helpless ex post. This is the novel situation that a legal definition of smart contracts needs to address. Unlike non-smart contracts whose performance can be stopped by the parties either voluntarily or by court order, once a strong smart contract has been initiated, by definition, it must execute. If, for instance, an individual in our above hypothetical were to install a device in his brain that would cause crippling pain if the lawn was not mowed, there is a case that the contract is in a stronger sense self-enforcing. This is the novel question posed to courts, and so this article will examine this second set of contracts. Much of this article will deal with smart contracts whose execution is contrary to governing law.

Contractware

Contracts are most often enforced by the parties to the contract. This is because most contracts do not end in breach and rancor, but rather in performance and completion. Modern industrial society would

not be possible if this were not the case.

It is only when there is a dispute over a contract that there is a need for enforcement. Yet resorting to the court system is a resource-intensive process.[17] The opportunity to ensure performance ex ante is a preferable situation if the expected value of the costs of litigation outweigh the expected value of the contract. Because litigation can be a resource-intensive undertaking, the rise of contractware qua enforcer could be a welcome possibility.

I will define contractware as the physical instantiation of a computer-decipherable contract.[18] The terms of many contracts can be written in programming languages that are communicated to a machine.[19] The reason for this is that performance and enforcement of a contract essentially boils down to conditional statements, which are foundational to computing.[20]

For example, in a secured auto loan, if a certain amount of money is not received by a certain date, then the car can be repossessed. While many contracts are certainly more complex, at base, conditional statements stand behind all enforcement.[21] Whether interpreting private contracts, statutes, or the Constitution, American courts take a series of inputs, run them through a series of conditionals, and then have an executor to enforce their output. For instance, if a city tried to segregate its schools, a court would run this factual input through the conditional of Brown, viz. if segregation, then enjoin, and have someone enforce the output.[22]

It is important to mention that the instantiation of the contract need not be in a physical piece of property or hardware, but can instead be in another piece of computer code. For instance, a bank account could include contractware that interacts with the bank's systems. As an example, such contractware could commit a buyer to send money to escrow once certain external conditions were met. Automatic payment of credit card bills, such as the service offered by Chase, are already in operation.[23] As a technological matter, until the advent of computers, it was difficult to use contractware. This left a larger role for courts and their agents to enforce contracts. Now, however, with increased digitization and the so-called "Internet of Things," the feasibility of installing contractware has increased dramatically.[24]

On the above view, the enforcement of a contract is nothing more than the running of a circumstance through a conditional statement. The central question to ask is: who runs the conditional statement? The most common and least disputed enforcement of a contract comes from the parties themselves. Take the contract, "Max agrees to buy Whiteacre from Richard for 500 Krugerrands." The conditional can be written "If Max pays Richard 500 Krugerrands, then Richard will sign a piece of paper granting Max legal title to Whiteacre." In most instances, Max gives Richard 500 Krugerrands and Richard then signs the document granting him Whiteacre. The parties themselves interpreted and enforced the contract.

When things go wrong, however, a third party can be invoked to interpret and enforce the conditional statements. The most familiar example of such a third party is a common-law judge using his legal reasoning combined with his sheriff to physically enforce the output of the conditional statement. At base, the judge is nothing more than a computer who applies a series of rules to a set of facts and then instructs others to enforce his output.[25]

But judicial enforcement of contracts is not the only way that contracts can be enforced. Instead of having a judge interpret and enforce the statements, it is possible to have a machine do so. Such a machine would need to have two abilities. First, it must be able to render correct outputs from given factual inputs. Second, its output needs to be reified some way in the real world. The vending machine is the archetypical example of a self-executing smart contract. Vending machines have been defined as "self-contained automatic machines that dispense goods or provide services when coins are inserted."[26] In other words, they complete one side of a contract once unilateral acceptance in the form of money tender has been effected.[27]

The contract at its most essential can be written in the following way: "Seller agrees to release one can of Dr. Brown's Cel-Ray Soda if Buyer inserts one Krugerrand into this vending machine." The Seller here is not the vending machine, in contradistinction to our Whiteacre property sale, where Richard was the

Seller. Instead, the Seller is effectively outsourcing the contract execution, with the vending machine merely acting as his third-party distribution agent and enforcement mechanism. Buyer inserts his Krugerrand, and vending machine performs by releasing one Cel-Ray Soda.

During the transaction, the computer inside of the vending machine is presented with a factual situation, i.e. the insertion of a Krugerrand and selection of Cel-Ray as the Buyer's choice. Next, the vending machine applies the contractual rules to the instant case, leading to a judgment output, i.e. dispensing one Cel-Ray Soda, which is the benefit of the bargain. The computer then directs the physical mechanisms of the vending machine to enforce the contract between the Buyer and the Seller. Had the factual situation been slightly different, for example Buyer inserted a penny, then our computer-judge would have rendered a different output and would have directed the vending machine to a different action, i.e. returning the penny without dispensing the Cel-Ray Soda.

One reason for the existence of contractware may be the lowering of costs through the ensuring of performance without recourse to the courts.[28] As we will be shown now, another reason may be the subordination of state authority to individual autonomy. The vending machine demonstrates this clearly in both its utilitarian and utopian purposes.

The Radical History of the Vending Machine

The first known reference to a vending machine came in 215 B.C. in Pneumatika, a book by the Greek mathematician, Hero.[29] In it, he detailed a machine that dispensed holy water for use in Egyptian temples. The user would put a coin in a particular spot, which would trigger a lever that opened a valve that dispensed the water.[30] Fear of divine retribution would combat the use of fake coins.

Although coin-activated snuff and tobacco boxes were used in England in the 17th century, one of the most conceptually important early uses of vending machines was as a means of evading censors.[31] The British bookseller, Richard Carlile, invented a book-dispensing machine so as to avoid prosecution under the country's libel and sedition laws.[32] He had been jailed previously and wanted to avoid any future liability, so the idea was to make it impossible for the Crown to prove that any individual bookseller actually sold the blasphemous material.[33] He argued that it was purely a contract between the buyer and the machine with the publisher having no formal involvement.

Here is Carlile's description of the machine as it appeared in The Republican:

Perhaps it will amuse you to be informed that in the new Temple of Reason my publications are sold by CLOCKWORK!! In the shop is the dial on which is written every publication for sale: the purchaser enters and turns the hand of the dial to the publication he wants, when, on depositing his money, the publication drops down before him.[34]

The Crown, however, was not amused. Use of the device was ineffective and both Carlile and his employee were convicted of selling blasphemous literature through the device.[35] Although unsuccessful in this instance, the vending machine demonstrated its ability both to help achieve political and economic ends.[36] The fact that Carlile flaunted his attempts to evade prosecution would make this an easy case for the court, but this article—discussed below—will deal with the theoretical question of how a court should approach a less flagrant smart contractor. Before moving onto this question, a second technological advancement will be highlighted.

Decentralized Ledgers

As mentioned above, contractware solves the problem of performing contracts by eliminating the human element ex post. From a technical sense, if nothing intervenes to prevent the machine from working, then, by definition, it will ensure performance. Yet a machine owned by one of the parties of a contract does not solve the problem of interpreting or writing the contract. The problem, briefly stated, is that an independent third party must interpret the contract in accord with the intentions of the parties.[37] This is a problem that public courts often try to solve. Another solution to this problem is blockchain technology.

A blockchain is a decentralized collection of data that is verified by members of a peer-to-peer network. [38] The concept most famously arose in the context of bitcoin, where the data collection is a ledger of time-stamped financial transactions. [39] The bitcoin blockchain, like all others, is a solution to the double-spend problem, a variation of the above problem of human interpretation and the possibility of judging one's own case. [40]

Modern industrial society requires trust. As an example, Americans generally trust that corrupt officials have not doctored the state's real property records. If a malicious county clerk were to forge a deed, it could cause all sorts of problems for bona fide property owners. Although this is not a huge problem in the developed world – indeed, our world is developed because this is not a huge problem – in countries with less of a commitment to the rule of law and property rights, property recordation is a problem. Citizens in other countries do not have such trust. [41]

Another example of faith that is placed in centralized institutions is in the banking system. Americans generally trust our banking institutions to keep an accurate reading of the balance on our checking accounts. While these banks have redundancies in the form of backup servers, they are still centralized institutions and, in some sense, judges in their own cases until brought before a court. If a bank asserts an individual has a balance of $1,000 and the individual claims a balance of $10,000, then a third party is likely needed to adjudicate the dispute.

This is what blockchains seek to solve: the problem of establishing consensus without the need for a centralized repository of information. Blockchains are decentralized collections of data. The unit of a blockchain is a block, which contains certain information, such as credits and debits or property ownership. A block is verified by a large number of computers in a network, called nodes, and then tacked on to the previously verified blocks. This chain of data blocks is known as a blockchain. [42]

A well-known blockchain is the Bitcoin blockchain; it encodes data that has a market capitalization of $9 billion as of August 28, 2016. [43] The data stored on each block consists of transactions, which are debits and credits to bitcoin accounts. "Murray paid Reuben 10 bitcoins on March 2 at 4 p.m." is an example of a transaction that would be recorded on the Bitcoin blockchain. [44] That block of data would then be verified by a large number of nodes and then tacked on to the previous chain, so that the blockchain would be one block longer. As it currently exists, the Bitcoin network has amassed the world's largest amount of computing power. [45]

What makes the Bitcoin blockchain novel is that it relies on a decentralized network to verify the data as valid according to a set of shared rules. Information already contained in a verified blockchain cannot be overwritten without reaching consensus with the entire network to propagate the altered information. So, while this is not to say that the invalid data cannot be posted, a strong effort is needed to do so. [46] In the case of a single bookkeeping instrument, all a malicious actor would have to do to credit himself a million dollars would be to gain access to the instrument. The security of the Bitcoin blockchain and other blockchains is beyond the scope of this Article. Although this has been borne out by recent history, it is an assumption of this paper that individuals will trust blockchains. [47]

The implications for the smart contract are that terms of the contract and the state of facts relating to the performance of the contract can be programmed into a decentralized blockchain that cannot be overridden by any individual malicious or mistaken node. If millions of computers verified that "Murray paid Reuben $100 on March 2 at 4 p.m." and these computers are disinterested and do not make computational mistakes, then one can assume with an exceptionally large degree of certainty that Murray did, in fact, pay Reuben $100 on March 2nd at 4 p.m. [48]

The implications are vast. [49] Stock recordation, corporate governance, and auditing have all been proposed as areas where blockchains can increase efficiency. Whether the benefits of adopting blockchains outweigh the costs of doing so is beyond the scope of this article.

The starter interrupter combined with a decentralized ledger offers a powerful example of the combination between these two technologies. Instead of programming the contractware so that its inputs and outputs are determined and executed by the creditor's software, a car's contractware can be

programmed so that its inputs and outputs are determined and executed by a neutral blockchain. Suppose the relevant term of the contract is that "If Murray does not pay Reuben $100 by March 2nd at 4 p.m., then Murray's car will be rendered immobile, and Reuben can repossess." The contractware will search the blockchain for such a transaction, and if it finds it, will allow the car to start. If it does not find such a transaction, it will prevent the car from starting. Neither of the parties must trust the other for the contract to be performed. They must trust the disinterested blockchain, which is capable of enforcing the relevant terms.

The contractware reifies the terms of the contract in such a way that technology can compel performance. The decentralized ledger ensures that such contractware operates in an independent manner, free from the problems of self-help. It therefore makes sense to call it a smart contract because it is able to do more than a traditional contract. It can endogenously enforce an ex ante bargain (contractware) and can also allow neutral, third-party enforcement (decentralized ledger).

History of the Idea and Some Preliminary Observations

Smart contracts have existed long before they were consciously described as such. They are the result of human action, not human design.[50] This means that contracting parties were incentivized to lower costs without consciously heeding the advice of academics.[51]

Smart contracts were first described by lawyer and technologist, Nick Szabo, in 1997.[52] Szabo defines smart contracts as contractual clauses embedded into hardware and software in such a way that makes breach more expensive.[53] He provides two examples: vending machines and devices for repossessing automobile-collateral. By decreasing the costs of mediation, self-enforcement, and arbitration, Szabo saw smart contracts as representing a fundamental shift in the world away from paper and towards digital systems, like the banking backed by computers and digital databases.[54] This shift was not to take place immediately, however, as Szabo recognized the value of the "long history" of paper.[55]

Long before Szabo, however, financial institutions were using computer code to facilitate transactions, like options contracts and bookkeeping.[56] The real breakthrough for smart contracts came with the advent of bitcoin and the proliferation of blockchain technology. First proposed in 2008, the Bitcoin protocol was a successful experiment in the mass usage of decentralized ledgers, which form an important basis of smart contracts.[57]

The proliferation of decentralized ledgers led to a new discussion of using technology to enforce agreements between individuals without recourse to third parties. New companies and protocols have aggregated the essential code to write smart contracts. This code exists apart from the bitcoin ecosystem. These new companies are building an ecosystem for experimentation with an implementation of smart contracts.[58] There has been a proliferation of writing about the subject, mostly from a technical or financial perspective.[59]

Place in Existing Contract Law

A contract is a legally enforceable agreement.[60] The novel issue of smart contracts is what happens when an agreement can be enforced not by public law enforcers, but through the terms and mechanisms set forth in the terms of the contract itself. The typical legal action for breach of contract involves an aggrieved party going to a court of law or equity to demand money damages, restitution, or specific performance.[61] With a smart contract, the aggrieved party will need to go to the court to remedy a contract that has already been executed or is in the process of being performed. This is because, by definition, a strong smart contract is already executed or in the process of being executed by the time the court hears the case. So the remedy must come after the fact to undo or alter the agreement in some way.

The three phases of contract law this section will address are formation, performance, and breach. Each of these phases will be covered to understand how these new contracts can be placed in the context of traditional doctrines and concepts.

Formation

The initial stage of a contractual agreement is not markedly different between smart and traditional contracts. This is because before any contractware can operate, two parties must agree to some set of terms that initiates the program.[62] In the realm of smart contracts, unlike traditional contracts, acceptance comes through performance. An individual can say they will initiate a smart contract, which may be a contract in regular law, but until the program initiates, there is no smart contract. Smart contract code can be posted to a ledger as an offer though. Once an action is taken to initiate acceptance, such as by ceding control over a certain amount of money to the code, the contract is formed.

Just as there is bargained-for consideration in a traditional contract, there is consideration in a smart contract. One of the reasons for have the doctrine of consideration is that courts believe that mutuality of obligation distinguishes a contract from a gift, for which parties do not have the same rights of legal enforcement.[63] As will be shown below, where a gift induces action, that action can serve as a substitute for consideration.[64] Smart contracts have the potential to formalize the instances where courts will allow contracts to be enforced. This is because the terms of the smart contract are explicitly laid out and each side's obligations and benefits are immediately apparently.

In a contract, the bargain can be presented unilaterally, like a vending machine, or can be bargained-for as in the terms of a loan agreement.[65] But what happens in a smart contract when there is no consideration? A foundational contracts case will be analyzed through the lens of both traditional and smart contracts.

In Ricketts v. Scothorn, a grandfather promised to his granddaughter a sum of money, inducing her to quit her job. The grandfather dies and the executor of the estate refuses to pay her.[66] The granddaughter brought an action against the executor of his estate, claiming that she relied on the grandfather's promise. The court held that the daughter could recover money damages because she detrimentally relied on the promise of her grandfather.[67]

But imagine a situation where the grandfather wrote into the gift-promise code that he or his estate could retain the right to change his mind or explicitly wrote into the code that he or his estate could not change his mind. This would be done using a smart contract. In this instance, it would be impossible for the grandfather to change his mind if the computer program did not allow for a change. The grandfather then writes the terms of this gift-promise into computer language that is readable by his bank including terms that do not allow for revocation.

An ability to write into the code options to change one's mind or the mind of one's assignees would make the doctrine of detrimental reliance less important because recipients of gifts could demand that their gifts come with a promise of finality; thus, the ability to recant the promise becomes a disclosed term of the contract. In Ricketts, it is likely that the grandfather would have happily tied his executor to the mast. If the counterparty did not give this additional promise in the code, then the gift recipient would be able to act accordingly; if the counterparty did give the promise, rights are more clearly defined.

Smart contracts solve the problem of gift-promises by giving both the promisor and promisee the ability to encode finality so that parties can organize their behaviors around a mechanical certainty or lack thereof.

Instead of going to court to ask the state to enforce the contract, the parties can agree to a cheaper enforcement mechanism. This is the method by which smart contracts reduce transaction costs. In the realm of wills and estates, like in Ricketts, smart contracts can be of particularly high value because they will bind the hands of the executor to the will of the testator, with little room for deviation.

Some of the most difficult problems of early contract law involved defenses of misunderstanding and mistake.[68] With respect to interpretation, the use of computer code has the potential to minimize future conflicts over terms.[69] In Raffles v. Wichelhaus a controversy arose over a cotton shipment contract

when two ships named Peerless could both fulfill the terms; one party claimed he intended one ship, the other party, the other.[70] Such problems are virtually non-existent now, at least in the shipping world, but for similar problems that may exist, the precision of cryptographic identifiers is able to dispatch with such issues.[71] Although ambiguity certainly exists in programming languages, these ambiguities are less than in the real world because of the fact that there are simply fewer terms that a computer can recognize than a human can recognize.[72]

Ambiguity is celebrated in human language. It is a central feature of literature, poetry, and humor. Ambiguity is anathema to computer language. An ambiguous computer language is a nonsensical concept because the predictability of computers is what gives part of their value; imagine a computer that was asked, "what is 1 and 1" it randomly returned either "two" or "11". Although it is debatable whether every contract can be translated into machine language, many of them can be.[73] When lawyers or the programmers they hire write contracts in code, there is less of a chance for ambiguity than in natural language if only for the simple fact that artificial language must be complete and predefined, whereas natural language is infinite.[74] That is to say a person can walk around and verbally recite lines of code and people can at least understand what he is saying; a machine cannot understand human language that it is not programmed to understand. All of this is simply to say that the problem of ambiguity is reduced in the smart contract context.

Finally, all of the usual defenses to formation of a contract also apply in the realm of smart contracts, although as will be seen later, enforcing the remedy against a strong smart contract may prove problematic to a court. Take unconscionability and illegality, for instance. If a vending machine were to sell alcohol to minors or sell alcohol in a dry jurisdiction, then the contract could be voided as illegal.[75] As will be discussed, the remedies will be either ex post through legal action or ex ante through regulation. In this instance, the illegal contract can either be policed through a prohibition on alcoholic vending machines[76] or a system of preclearance where a driver's license scanner or some mechanism are required to ensure compliance with age requirements. Similarly, suppose the vending machine charged $1,000 for a can of Coke and a court were to find this to be substantively unconscionable. The remedies would again either be in damages or in policing the use of such vending machines before the contract could be formed.

Because the possibility of policing and damages exist, the issues of contract formation are largely the same in the traditional and smart contract world. The main difference is in the precision with which terms can be defined and inserted. Ambiguities must be taken care of by a functioning program and there is no "I do not know." The history of computing shows that programs do not always operate as their designers expect, but when code is executed, the code does operate.[77] Although the actual output of a smart contract may differ from the intentions of the parties, this system provides a more optimal first approximation. This is because computer code can be predicted according to a set of rules, whereas the ambiguity in human interpretation is less robotic by definition.

Performance and Modification

A contract can be performed, modified, or breached. This section addresses performance and modification issues.

The performance phase is made easier with smart contracts as they offer a tool to solve ambiguity problems addressed above. A potential problem here, however, comes with imperfect performance. Courts in the United States do not demand perfect performance for a contract to be recognized and enforced.[78] The common law doctrine of substantial performance permits a contract to be recognized even if the performance does not fully comport with the express terms laid out.[79] This is the kind of leeway that a computer program cannot recognize because it involves an outcome that was not contemplated and specified by the parties. Imagine, for instance, a contract for a painting that is contingent on the reasonable personal satisfaction of the buyer. One way parties can deal with this is by baking in a certain degree of discretion into the terms of the contract initially or by simply not using a smart contract if discretion is a necessary part of the contract. However, if the terms were to diverge

from what the law recognizes, the law would have to again decide between ex ante and ex post solutions to the problem.

Most conceptually challenging, however, is how smart contracts will deal with modification. The law recognizes certain excuses that will absolve a party from performance or require some sort of modification.[80] Impossibility and impracticability are two such excuses. When a contract becomes illegal after it is formed, then the parties can be excused from performance and there is generally no remedy for an aggrieved party.[81] This poses a problem for the smart contract.

There needs to be a method by which smart contracts can be updated to incorporate changes that may be required by the evolving legal landscape. Suppose that at the time of contract formation, the time a debtor needs to be in default for the creditor to repossess is 30 days and that after the contract is executed, a legislature changes the law requiring that time period to be 90 days.[82] There are numerous ways of addressing this situation, ranging from state-backed to purely private. One method could be a system in which the relevant jurisdiction creates a publicly available database and application programming interface (API) of relevant legal provisions. These would be provisions related to the terms of the contract. The smart contract would call these terms and would be able to update those provisions terms in accord with the jurisdiction's update of the database.[83]

Another method would be through ex post policing of the parties; this puts the burden on the parties or their agents to update the code. The benefit of this option is that there is no need to rely on the third-party government to create a new infrastructure, while the downside is that the parties themselves can potentially unilaterally change the terms of the contract, which is one of the problems smart contracts try to rectify. This could be obviated by leaving certain terms of the contract modifiable, while restricting others from modification. That payment is necessary could be an immutable term, whereas the length of time a debtor has before he is in default could be modifiable. This suggests that government API's may have a master override over contract terms, which reflect the application of prevailing law over contracts in certain circumstances.[84]

Finally, computer programs are regularly written with the option of inserting code later. Only those contracts that would involve some kind of irrevocability would force courts' hands. This is because a court would be tasked with enforcing a law that would override the terms of the contract; there would be conflicting dictates. Party autonomy does not trump all other values in state-based legal systems.

Enforcement, Breach, and Remedies

The central problem in the final question of contract law is what happens when the outcomes of the smart contract diverge from the outcomes that the law demands. Above are numerous examples where the technical outcome of the smart contract would not be permitted by a court under existing law, e.g. the heroin vending machine.

As a threshold, it is possible that contract law and the actual written contracts would have influence on each other so as to minimize these divergences. Courts are going to be more likely to enforce smart contract terms because the courts will have more certainty as to party intent because the parties explicitly laid out their terms. Smart contracts drafters are going to be more likely to write smart contracts that comport with extant law and write terms that are variable to accommodate future changes in the law. The terms of a lease, for instance, will change to accommodate the property law of the jurisdiction. Additionally, torts could emerge for negligent coding or negligent update that would further ensure smart contracts are drafted in accord with existing legal standards. But what happens when these forces are not enough to overcome the divergence?

It is a good rule of thumb that the entity with more guns wins. Here, governments generally have more guns than private parties and so the state's courts are in a position of enforcing their law over the private law. Enforcement either occurs before or after the damage has occurred. This damage is not to either of the contracting parties because they are getting, by definition, their bargain.[85] Instead, the damage is done to the exogenous laws of the society and not the parties themselves.[86] If two parties contract to buy liquor, both are satisfied with the bargain ex ante. If one of those parties is below the drinking age,

he is still satisfied with the bargain. The only one ex ante not satisfied is the government and the government is in a position to respond to that dissatisfaction in some way.

In the United States and other common law systems, ex post enforcement is the preferred system and there are many reasons to believe why this is a system conducive to greater prosperity and vibrancy.[87] In the sections below this article will discuss the merits of these two positions, but here it suffices to say that the two likely categories are regulation/policing and criminal/civil actions. There is a spectrum on which these remedies should be offered. In the United States, it is the exception that the government bans certain objects because their possession is per se problematic for society. Automatic weapons and child pornography both fall into this category.[88] If the government does not take this tack, then it is largely left with ex post enforcement.

Some unenforceable contracts result in criminal prosecutions, while some result in non-enforcement.[89] It is too speculative at this point to see how the governments will respond to smart contracts because these technologies have yet to reach a level that requires a government response. They may not reach this level because individuals may not want to change their current contracting patterns because they are fine with the level of leeway and ambiguity that currently exists. It is unlikely, for example, that individuals will want to implant mini-bombs in themselves to ensure compliance with credit card payment. Because egregious bargains like those using the mini-bomb are unusual, it is likely that responses to unenforceable private contracts will remain in the ex post phase and tend towards civil, not criminal enforcement.

It will be helpful to solidify the above discussion in a law that is embryonic, but at least extant: starter interrupters.

Case Study: Starter Interrupters

The existence of a public court system is the antithesis of private self-help because the parties seek external recourse from a third party.[90] There are reasons for this, including a desire to prevent might from making right.[91] But recourse to courts is not without its costs.[92] Forcing a landlord to go through a lengthy eviction process raises the costs for non-breaching tenants, for example.[93] The situation is similar to when automobiles are collateral. In an attempt to increase recovery rates for their collateral, automobile lenders have turned to using devices called starter interrupters.[94]

Starter interrupters are an archetypical example of a smart contract and how the law deals with them is instructive in crafting appropriate legal regimes. A starter interrupter is a device that is installed in an automobile that allows for a remote party to prevent the engine from starting.[95] It allows a user who controls the starter interrupter to remotely shut off an automobile. These devices often also include global position systems, so that the collateral can be located.[96] The New York Times reported on an Arizona company, C.A.G. Acceptance Corporation, which offers its automobile loans on a condition that if the debtor is in default, the company reserves the right use the device to prevent the car from starting.[97] Such devices are estimated to be installed in over two million automobiles.[98]

There are a number of safeguards to the power of the starter interrupters that companies use to ensure that there are not egregious problems with their use.[99] For instance, a starter interrupter cannot disengage a car while it is currently running, which would have the obvious potential of causing accidents. The starter interrupter can be manually overridden with a code in certain instances in cases where life and limb are at stake. The creditor can give a sheet of a number overwrite codes, each of which can only be used once to prevent abusing the leniency for exigent circumstances. These common-sense exceptions to the power of the starter interrupters are included in best practices guidelines for the industry.[100] This would allow the companies to comply with existing law that prevents, for instance, tortious conduct on highways.

The cost of locating and then repossessing automobiles is a significant one and the starter interrupter, a form of contractware, is a powerful tool to drive down these transaction costs. This technology is currently being used and developed by creditors who are able to increase their collection rates by locating their collateral and preventing its misuse.

Some critics view such use by creditors to collect collateral as unfair to those debtors who rely on the collateral for transportation to work.[101] Other critics in response point to the lower interest rates that debtors can afford because of the increased rates of recovery and therefore the systemically lower credit risk.[102] This debate is beyond the scope of this article, but if there is an economic incentive for both creditors and debtors to use these devices, the law will be forced – and indeed has been forced – to determine the legality of their use.

Contract law is generally governed by states and there is no preempting federal law specifically dealing with starter interrupters,[103] but there is not much state law applicable to contractware. As one recent survey of the extant law concluded, "generally…SIDs [starter interrupter devices] may be legal in most states due to the secured party's right to the 'self-help' repossession provisions of Uniform Commercial Code ("UCC") section 9-609."[104]

Section 9-609 of the Uniform Commercial Code, as adopted in various forms by the states, governs self-help of secured creditors. The UCC gives a secured creditor the right to either "take possession of the collateral" or "render equipment unusable" without judicial process so long as the action "proceeds without breach of the peace."[105] A rich case law exists on what constitutes a breach of the peace, and as will be shown below, it will not be difficult to fit starter interrupters into this existing corpus.

California, Colorado, and Connecticut all explicitly affirm the legality of starter interrupters but place certain restrictions on their use.[106] The primary concerns of the state legislatures are both that the debtor has notice that the device has been installed and has a right to cure the breach.

The rights of debtors under the Bankruptcy Code add another wrinkle in the straightforward use of starter interrupters. A bankruptcy court in Arkansas ruled that the installation of a starter interrupter, while not per se illegal, violated the Bankruptcy Code's automatic stay because it prevented the debtor from the normal use of her car.[107] The court noted that the creditor could have remedied the situation by "taking action to ensure that Debtor had the correct code to operate her car each month, such as by mailing the correct code to Debtor each month."[108] A line of code written that would honor a court's grant of an automatic stay motion by allowing the car to operate is another potential remedy.

The automatic stay, like the prohibition on selling alcohol to minors, acts as an external condition that the smart contract must incorporate into its terms if it is to comply with the law. The reason is because an individual cannot contractually waive his right to file for bankruptcy as a matter of public policy.[109] As seen before, this can either be solved ex ante or ex post. This situation seems ripe for private solution, as it is not difficult to determine whether a party has filed for bankruptcy, given the public nature of these proceedings. A simple conditional could be written that if bankruptcy has been filed, then the starter interrupt cannot be engaged.

As blockchains currently exist, starter interrupters are operated by the creditor and done so with the use of discretion.[110] But large corporations, like Toyota, have contemplated using blockchains to enforce their contractual arrangements.[111] By invoking a blockchain for third-party verification, this discretion would be lost, but the debtor would be able to ensure that an interested party did not have the unilateral ability to control his collateral. The lower interest rates that come along with the blockchain's assurances may provide a valuable option to some debtors who view the rigidity as enticing.

Self-Help and Smart Contracts

Private Enforcement and Political Philosophy

Self-help remedies have been defined as "legally permissible conduct that individuals undertake absent the compulsion of law and without the assistance of a government official in efforts to prevent or remedy a civil wrong."[112] Automated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement. A smart contract may not, however, meet the first terms of the definition because of illegal contracts like the vending machine that dispenses heroin or the implanted bomb that explodes when a debtor defaults. These contracts are outliers that must be dealt with, but the background approach the state should take towards smart contracts is a liberal one.[113]

Smart contracts offer a wider range of assurances to parties who previously had to use other mechanisms to ensure performance. For example, without smart contracts parties are more likely to prefer instantaneous performance or overvalue the reputation of the counterparty. These are good proxies for ensuring performance, but not ironclad and come with their own costs.[114] Much of the literature on self-help in contract law has dealt with how a party who has been aggrieved can remedy the wrong that has been committed against him.[115] The advent and proliferation of the smart contract will focus the attention on the harms done to the breaching party, ensuring that party autonomy take a backseat to other norms that society wishes to enforce. In what follows, this Article will examine the potential benefits to non-breaching parties and society at large and then examine the costs to breaching parties and what limits the state will place on the use of smart contracts.

As with many new technologies, behind bitcoin stood a political ideology skeptical of centralized power and supportive of capitalism and free markets. Although he[116] never identified himself as such, many describe the creator of bitcoin, Satoshi Nakamoto, as a libertarian. Certainly many of the early adopters of bitcoin were self-described libertarians.[117] Szabo has been called libertarian and his writings emphasize alternatives to the state's enforcement of rights.[118] Traditionally, states have been defined as monopoly holders of force with a power to tax.[119] Among the most radical visions for smart contracts is that the technology will subject the provision of justice to market forces and break the state's monopoly over the court system. This is an idea that has been discussed by many libertarians, including Robert Nozick, Murray Rothbard, and David Friedman.[120]

For many libertarians, the purpose of civil government is to protect private property and enforce natural rights.[121] Most fundamental here is the harm principle that an individual should be free to do as he chooses, coterminous with the rights of others.[122] This implies a strict adherence to freedom of contract.[123] On this view, smart contracts use technology to enforce party autonomy in a more effective manner because they prevent external interference. If contractware progresses to a point where there is truly no need for third-party enforcement, there would be no need for a state and the attendant costs that many libertarians see as unjustifiable.

Smart contracts could be used to encode certain constitutional principles into armaments, such that weapons would not work if certain conditions were not met, e.g. if Congress does not declare war, weapons will not function on foreign soil. Although fanciful, applications like this limn the concerns animating many early proponents.[124]

This speculative and radical vision of smart contracts is not held by all proponents of the technology. Rather, some proponents are primarily focused on the capability of smart contracts to reduce transaction costs. Instead of fundamentally changing the nature of political governance, a new wave of smart contract proponents is concentrating on the idea that their use can make the economy and corporate governance more efficient. I call these individuals the Coaseans because they care about reducing transaction costs.[125] One of the main areas to do so is corporate governance within firms, where a number of proposals have been discussed.[126] These proposals include improving shareholding voting systems, tracking debt and equity issues, and enabling triple-entry accounting.[127]

An example of a firm that utilizes smart-contract technology to execute its corporate-governance rules is a decentralized autonomous organization ("DAO"). One way of thinking of a DAO is that it is an organization where the rules of management are predetermined and run on computers.[128] One such DAO was formed in 2016.[129] The idea was to create an investing entity that would not be controlled by any one individual, but by shareholders voting based on their stakes on a blockchain. This would reduce transaction costs by obviating the need for a management team.[130] The entity was funded with $150 million.[131] Soon after this money was raised, about $40 million of those funds were diverted from the organization by a "hacker" who used the code in an unanticipated way.[132] Strictly speaking, however, the hacker did not "hack" the code in a malicious way, but rather used the terms of the existing smart contracts to accomplish something others later found objectionable, i.e. the diversion of their money.[133] Consider this using a legal loophole to effect a result that was clearly within the letter of the law, but not within its spirit.[134]

Another example of smart contracts enabling novel corporate-governance procedures is the use of prediction contracts. A prediction contract is a binary option contract whose value is contingent on an event's occurrence.[135] These contracts are often cited as predictors of presidential elections, where market participants buy and sell contracts in accord with shifting beliefs in a candidate's probability of being elected.[136] But, they can also be viewed as a form of smart contract that can be executed on a blockchain without any input from a single third party. In many credit default swaps, for instance, a third party, the International Swaps and Derivatives Association, will determine whether a credit event has been triggered.[137] With a smart contract using a decentralized blockchain for authorization, a network itself can verify whether an event took place and whether the contract will pay out. This has applications in the realm of corporate governance, where decisions can be automated based on discrepancies between the option price and the stock price, directing a board of directors to take one course of action over another.[138]

Limiting Principles

The above has shown the benefits that come from judicial recognition and enforcement of smart contracts. Some of the believers in smart contracts think that these benefits can be appreciated without judicial recognition and enforcement because smart contracts can supplant traditional judicial systems enforced by a centralized state.[139] This section of the Article analyzes the positive question of where the outer-bound of a state's acceptance of smart contracts lies. Three examples along a spectrum will demonstrate the degrees to which states and their judicial systems can approach smart contracts. On the one end of the spectrum is permitting the use of smart contracts use and recognizing them in collateral matters, e.g. recognizing a smart contract when going through the probate process. On the other end of the spectrum is prohibiting the use of smart contracts or banning certain forms of contractware. Similar to the manner in which non-smart contracts cover a variety of different agreements – employment contracts are different from marriage contracts – smart contracts will likely be adapted to cover a wide range of subject matter. The application of a particular contract will likely be relevant to which attitude the courts adopt, much as not all non-smart contracts are the same; employment contracts are different than marriage contracts.

Starter interrupter devices are illustrative of the permissive side of the spectrum. As was shown, courts have recognized these devices as legitimate and allowed companies to use them to repossess vehicles, provided there is no violation to external laws, including the Uniform Commercial Code's "breach of peace" provision and the Bankruptcy Code.[140] How courts treat violations will likely be instructive. Suppose a starter interrupter is placed in a truck that is essential to a business. Instead of merely shutting the car off, this starter interrupter will permanently damage the car's engine, rendering it unusable, if payments are not received on time. Then, suppose the debtor files for Chapter 11 bankruptcy. The debtor-in-possession or trustee could charge that the use of the starter interrupter is a violation of an automatic stay, as it is an attempt by the creditor to control the property of the estate, even though the control is automatic and out of the creditor's hands.[141] The question then put to the court is whether starter interrupter can be used at all if they have such potential.

A second example in the middle of the spectrum, would be a modern version of Williams v. Walker-Thomas Furniture Co. In Williams, the court set forth a standard of unconscionability by asking whether the terms of a particular cross-collateralization contract were "so unfair that enforcement should be withheld."[142] Imagine, however, that the furniture in that case was installed with contractware that blasted an annoying siren if payment was not received. Further, imagine that this was explicitly agreed to by the debtor ex ante. A court bound by Williams, could easily deem the contract unconscionable. This would leave the court to determine the proper remedy. The court could award damages to account for the harms caused by the automatic execution of the contract, which damaged the collateral in an unacceptable way. In this instance, such a remedy seems appropriate because the damage is not irreparable. It is likely that what the court would do is create a new breaching the of peace doctrine that creditors and the contractware would have to abide by.

The final, and most egregious, example is contractware installed into humans. Although certainly a dystopian gedankenexperiment, it is worth imagining a scenario where creditors can install devices into

the bodies of debtors and have the device force them into slavery or some state of impaired consciousness if they default. Such a scheme would certainly be unconstitutional as a violation of the Thirteenth Amendment even if the debtors supported the scheme as a way of securing lower interest rates. This is not the interesting question, however. What is worth analyzing is how a court would deal with such installation. Despite consent by each party, the court would likely nullify the contract. But will the court prevent the installation of the contractware into the body? Much more likely than judicial intervention is a legislative solution. States can and have banned objects that are not per se violative of rights, but pose an unacceptable risk to the morals of the community.[143] This can be a legitimate exercise of the police power of the state, such as, for instance, when the government bans the private possession of bazookas.[144]

What the above illustrates is that smart contracts exist in preexisting legal structures that do not unequivocally value party autonomy with respect to the formation and performance of contracts. The central question, however, is whether the state can use prior restraint to prevent the formation of contracts that have the potential to become contrary to public policy, but are not necessarily contrary to public policy themselves.

The likely answer is yes. It is hard to imagine a state sitting idly by while devices are installed to self-enforce contracts that are contrary to the state's own interests and policies. Although, the proposition is not black-and-white. When dealing with any question of prior restraint, the magnitude of the mischief must be weighed against the likelihood of its occurrence. The Supreme Court's First Amendment jurisprudence provides a useful model; n that realm, the Court has erred on the side of respecting autonomy and policing ex post.[145] In this instance, contractware ought not be analyzed in toto, but discrete devices and software applications should be evaluated. This evaluation should be based upon the rights implications, as opposed to the particular functions of the contractware device. So, while devices that prevent the usage of personal property could be allowed, implants that enforce unconstitutional contracts or contracts that are unconscionable or void against public policy would not be permitted.

These are questions for judges to decide on a case-by-case basis.[146] Common law principles ought to form the background of such analysis.

Conclusion

The creators of smart contracts have invited society to a party they are throwing. They say that this party has better food, booze, and music than the party being thrown down the street. But the other party has all of the people, even if the amenities are not as good. Whether society shows up to this new party is an open question. This is because legacy systems exist for a reason. By definition, they work. Both switching costs and uncertainty stand as barriers to the adoption of any new technology. Yet if the value of the new technology is overwhelming, such a change is more likely to occur.

One way of reducing uncertainty is by situating the new in the old. While there may be many barriers to the adoption of smart contracts, legal uncertainty need not be one of them. Courts need not upend extant jurisprudence to accommodate smart contracts.

Max Raskin

*At the time of writing, author was a fellow at the NYU Law Institute of Judicial Administration. B.A., New York University; J.D., New York University School of Law. For signaling purposes and for help on the paper, I would like to thank Oren Bar-Gill, Will Baude, Richard Epstein, Dan Evans, Ian Grigg, Andrew Hinkes, Mario Rizzo, Nick Szabo, David Yermack, the Mechanic's Liens Steering Committee, the NYU Austrian Colloquium, and the NYU Law Classical Liberal Institute. All errors contained herein are my own, except any egregious ones that may exist. In that case, I blame the aforementioned for their laxity in review. Cf. D.C. Makinson, Paradox of the Preface, Analysis 25, 205-207 (1965); see also Robert Bork, The Antitrust Paradox, xvi (1978).

Related

"Smart Contracts": A Smart Way to Automate Performance
April 2017
In "FintechExplainer"

Insurtech: An Industry Ripe for Disruption
April 2017
In "Legal News"

A New Journal at the Intersection of Law and Technology
November 2016
Similar post

Articles
Vol. I, Issue II (2017)
ZZZ-Featured Article
Tags: Blockchain, Fintech, Smart Contracts