Smart Contract Law:
The Promise and Limits of Self-Enforcement Through Contractware and Blockchain Technology

Max Raskin

Introduction .................................................................2

Smart Contracts Explained ...............................................4

Contractware ...............................................................5

Decentralized Ledgers ....................................................8

Situated in Extant Contract Law ......................................12

Formation, Defenses, and Interpretation ..........................12

Modification ................................................................12

Enforcement, Breach, and Remedies ...............................13

History .........................................................................14

Starter Interrupters ........................................................14

The Good ....................................................................17

Libertarians ..................................................................17

Coaseans .....................................................................17

The Bad and the Ugly ....................................................18

Three Examples ..........................................................18

Limiting Principles .......................................................20

To the Colloquium:

1 Nick Szabo, David Yermack
Thank you for inviting me to present an early draft of this paper. I am still thinking through many of the issues here and focused this draft on explaining the mechanics of smart contracts. There is much more involved and I would like to see what topics might be discussed in the analysis section that I have not considered. As such, the paper is front-loaded.

Introduction

The purpose of this note is to explain self-executing smart contracts and to situate them into the currently existing law of contracts. We can innovate our technology without innovating our jurisprudence.

The article begins with an explanation of smart contracts. There are two necessary technological components to this explanation: decentralized ledgers and contractware. A decentralized ledger, also known as a blockchain, is a database of information that is created by a network with no central authority. Instead of a system of public recordation that exists on the files of the town stored in city hall, a decentralized ledger keeps accurate information that is stored on the computers of anyone running the software. The second component is contractware, which the article will use to refer to the physical instantiation of contract terms onto pieces of property involved in the performance of the contract. A simple example of this would be a vending machine. Inside the machine is a physical device that is encoded with a contractual offer of the seller. The machine will only dispense a soda if the terms of the agreement are met, for instance, by depositing a dollar into the device. It is the combination of these two components that has made possible smart contracts that are enforced not by one party, but through a decentralized, third party network.
The next section of the article will analyze smart contracts through the lens of existing doctrines in contract law. It will go through the classic stages of contract formation and pose a series of observations and questions that are implicated by smart contracts. Consideration, formation, avoidance, performance, and remedy will all be discussed.

To concretize the discussion, the following section will explore one existing application of smart contracts: starter interrupters. These are devices installed in cars by creditors, allowing the creditor to remotely disable the vehicle if the debtor has breached the terms of the agreement. How courts and legislatures have dealt with these devices will be the subject of this section.

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 innovation can radically alter the nature of society and its relationship with the traditional centralized state. One of these beliefs is that private enforcement of contracts can ameliorate the need for monopolized legal services provided by the state. Some have contended that such technology could obviate that need. Like many technologies, however, the early vision of the first movers often gives way to the realities of a world that looks askance at revolution. On the other end of the spectrum are the benefits of smart contracts that do not upend the existing social order, but instead decrease transaction costs, allowing for industrial society to operate more effectively. This promise extends to financial transactions, corporate governance, financial products, and a host of other potential applications that have been analyzed by economists.

These benefits must be viewed in light of the inherent limits of smart contracts. The following section of the paper gives both a philosophical and practical set of problems with self-enforcing contracts. Briefly stated, there will always need to be a third party to enforce a
contract. What a smart contract does is ask both parties to tie themselves to the mast like Ulysses and *ex ante* commit to abiding by the terms of the contract. Given the strength of the contractware, it may be impossible to take oneself down from the mast. This is where the existing judiciary will step in. Because the state may categorically disapprove of the terms of a smart contract and may be powerless to alter performance *ex post*, it is possible that the state could ban certain forms of smart contracts and the contractware that enables them. It is possible, in other words, for the government to deem certain forms of property *per se* unconscionable even if both parties wish to tie themselves to the mast.

The article will then conclude.

**Smart Contracts Explained**

Smart contracts have existed long before they were consciously described as such. They are the product of human action, not human design.² By this we mean that businessmen did not heed the advice of academics who suggested ways of lowering transaction costs, but instead were incentivized to do so on their own. Like much of the common law, the legal and academic reaction to technological progress is exactly that, a reaction.

We will therefore first begin with an explanation of the mechanics of smart contracts using two essential concepts. Then, we will show historical examples of smart contracts in use.

---

² Adam Ferguson; Hayek http://oll.libertyfund.org/groups/104
Contracts are most often enforced by the parties to the contract. This is because most contracts do not end in breach and litigation, 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. Given the opportunity *ex ante* to ensure performance in accord with each party’s understanding of the contract is a preferable situation. It the resource-intensity of our court system that gives rise to the possibility of contractware.

We will define contractware as the physical instantiation of a computer-decipherable contract. The terms of many contracts can be written in a programming language that is communicated to a machine. The reason for this is that performance and enforcement of a contract essentially boils down to a conditional statement, which is one of the bases of computer programming. 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 complicated than this, at base, conditional statements stand behind all enforcement. 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 it through the conditional of *Brown, i.e. if* segregation, then enjoin, and have someone enforce the output.

---

3 Szabo (2001) has termed them “proplets.”

4 See e.g. [http://szabo.best.vwh.net/contractlanguage.html](http://szabo.best.vwh.net/contractlanguage.html); Composing contracts: an adventure in financial engineering Simon Peyton Jones (2000); [http://gavwood.com/Paper.pdf](http://gavwood.com/Paper.pdf); Ethereum
As a technological matter, until the advent of computers, it was difficult to use contractware and so much enforcement was done by courts and their agents. Now, however, with even refrigerators containing software, the possibilities of installing contractware increase dramatically.

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, but least exciting 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 that “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 often steps in to interpret and enforce the conditional statements. The most familiar example of such a third-party is a 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.

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. That machine would need to have two abilities. First, it needs to be able to give correct output
A vending machine is the archetypical example of a self-executing smart contract. 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.” It is important to note that the Seller here is not the vending machine, in contradistinction to our Whiteacre property sale, where Richard was the Seller. Instead, the Seller is in another location, with the vending machine merely acting as his third-party enforcement mechanism. Buyer inserts his Krugerrand and vending machine performs by releasing one Cel-Ray Soda.

What is going on in this enforcement is that the computer inside of the vending machine is presented with a factual situation, i.e. the insertion of a Krugerrand. Next, the vending machine applies the contractual rules to the instant case, leading to a judgment output, i.e. dispensing one Cel-Ray Soda. 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 have directed the vending machine to a different action, i.e. returning the penny without dispensing the Cel-Ray Soda.

Analyzing contracts through the prism of machine-decipherable conditions is a relatively new concept and the extent to which it is a comprehensive theory of contracts is beyond the scope of this article. For our purposes, there is only one essential point about contractware: it exists. One reason for its existence may be the lowering of transaction costs through the ensuring of performance without recourse to the courts. Regardless, however, parties have used the
technological advancement of contractware to program into pieces of physical property the terms of their bargained for agreements.

Decentralized Ledgers

As mentioned above, contractware solves the problem of enforcement. From a technical sense, if nothing intervenes and prevents the machine from working, then it will, if operating properly, enforce the contract. Yet a machine owned by one of the parties of a contract does not solve the problem of interpreting the contract. The problem, briefly stated, is in having an independent third-party interpret the contract in the correct way, a problem public courts often try to solve. Another solution is blockchain technology. We will first briefly explain the blockchain, then describe the problem it solves, and then investigate the technology further.

A blockchain, for the purposes of this article, is a decentralized collection of data that is verified by members of a peer-to-peer network. The concept first arose in the context of bitcoin, where the data collection was a ledger of time-stamped transactions.

For many, bitcoin refers solely to a digital currency that has fluctuated wildly, but behind the currency, stands a blockchain. The bitcoin blockchain, like all others, is a solution to the above problem of judging one’s own case.\(^5\)

Modern industrial society requires trust. As an example, Americans generally trust that the state’s real property records have not been doctored by corrupt officials. If a malicious county clerk were to forge a deed, it could cause all sorts of problems for \textit{bona fide} property owners. Although this is not a huge problem in the developed world – indeed our world is developed \textit{because} this is not a huge problem – in states with less of a commitment to the rule of law and

\(^5\) \textit{Nemo judex in causa sua}
more corruption, property recordation is a huge problem. Citizens in other countries do not have such trust.\(^6\)

Another example of faith we place in centralized institutions is in our 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, they are centralized institutions and, in some sense, judges in their own cases until brought before a court. If a bank says 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 the problem that blockchains seeks to solve: the problems caused by centralized repositories 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 to accounts 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.

The most well-known blockchain is the bitcoin blockchain. 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.\(^7\) That block of data would then be verified by a large number of nodes and then tacked on to the blockchain, so that the blockchain was now one block longer. As it

---

\(^6\) Honduras to build land title registry using bitcoin technology http://in.reuters.com/article/usa-honduras-technology-idINKBN001O01V720150515

\(^7\) Of course the block would not include the proper names “Murray” and “Reuben”, but rather their public addresses.
currently exists, the bitcoin network has amassed the world’s largest amount of computing power.

What makes the bitcoin blockchain unique is that it relies on a decentralized network to verify the data as not being faked. This is not to say that the data cannot be faked, but rather that there is no single point of failure. The security of the bitcoin blockchain and other blockchains is beyond the scope of this paper. Although this has been borne out by recent history, it is an assumption of the proliferation of this technology that individuals will trust blockchains.

The implications for the smart contract are that terms of contact 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 $10 on March 2 at 4 p.m.” and these computers are disinterested and not able to make basic mistakes, then we can assume with an exceptionally large degree of certainty that Murray, did, in fact, pay Reuben $10 on March 2 at 4 p.m.\(^8\)

The implications are vast.\(^9\) Stock recordation, corporate governance, and auditing have all been proposed as areas where blockchains can increase efficiency. Whether the benefit of adopting blockchains outweigh the costs of doing so is beyond the scope of this article.

The majority of the paper will discuss the implications of combining contractware with decentralized ledgers. A smart contract does not need to refer to a blockchain for verification, but could refer to protocols maintained by a centralized state. Combining the two, however, has been

\(^8\) It is worth noting that it is possible to instantaneously transfer from U.S. dollars into bitcoins, such that there is an identity between $10 and some amount of bitcoins that would actually be recorded on the blockchain.

\(^9\) Yermack
one of the promises and reasons behind the development of smart contracts as they are currently existing.

With the above in mind, we can now briefly solve some of the problems many have with the starter interrupter. Instead of programming into the contractware that its inputs and outputs would be determined and computed by the creditor’s software, a car’s contractware can be programmed so it will get its inputs and outputs would be determined by a blockchain or perhaps by protocols maintained by a court or legislature. Suppose the relevant term of the contract is that “If Murray does not pay Reuben $10 by March 2 at 4 p.m., then Murray’s car will be rendered unworkable and Reuben can repossess it.” The contractware will search the blockchain for such a transaction and if it finds such a transaction, will allow the car to start, and if it does not, will prevent the car from starting. Neither of the parties must trust the other for the contract to be performed. They must merely trust the disinterested blockchain, which is capable of enforcing the relevant terms.

Thus, a smart contract is nothing more than a combination of these two important technologies. The contractware instantiates the terms of the contract in such a way that technology can compel performance. The decentralized ledger ensures that such contractware operates in a just manner, free from the problems of self-help. It therefore makes sense to call it a smart contract because it is smart both with respect to its ability to be enforced with respect to the ex ante bargain (contractware) and its ability to enforce itself (decentralized ledger).
Formation, Defenses, and Interpretation

The initial stages of a contractual agreement are not markedly different between smart and traditional contracts. Like there is bargained-for consideration in a traditional contract, there is consideration in a smart contract. This consideration can be presented in a unilateral fashion, like the vending machine, or can be bargained-for as in the terms of a loan agreement between a creditor and debtor.

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 may prove problematic to a court. 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.

With respect to interpretation, the use of computer code has the potential to minimize future conflicts over terms. 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. Because human-readable contracts can be written in computer programming language, these human-readable contracts are necessarily going to include a greater chance for ambiguity than contracts that are only computer-readable.

Modification

Sometimes the terms of contracts must be changed, which would seem to pose a problem for the smart contract, which has been analogized to Ulysses tying himself to the mast. The first
point to note is that programs are regularly written with variable terms that will be filled in later. Suppose the at the time of contract formation, the time a debtor needs to be in arrears for the creditor to repossess is 30 days and that after the contract is executed, a legislature comes in and says that that time period should now be 90 days.

There needs to be some method by which the evolving legal landscape can be updated in the terms of the contract. There are numerous ways of doing this, ranging from state-backed to purely private. One potential method could be devising a system by which the relevant jurisdiction creates a publicly available database and application program interface (API) of relevant legal provisions related to the terms of the contract and that a smart contract would call these terms and have provisions for updating the terms in accord with the updating of the database. Another method would be through *ex post* policing of the parties; this puts the the burden on the parties 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 others not.

**Enforcement, Breach, and Remedies**

This section will focus on breach and remedies because the great virtue of smart contracts is that they are self-enforcing. The difficulty comes when the terms to be enforced are either deemed by the parties or the government to be enforceable.

- Efficient Breach and Liquidated Damages
- Unconscionability and public policy limit on smart contracts
History

- Satoshi and Szabo
- History of Vending Machines; from Hero of Alexandria; *American Vending Machines: A Social History*\(^\text{11}\)
- Subway Tokens/EZ Pass case study

**Starter Interrupters**

Starter interrupters, also known as starter interrupt devices (SIDs), are an archetypical example of a smart contract and how the law deals with them is going to be instructive into 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. It allows someone who controls the device to remotely shut off an automobile. The *New York Times* reported on a company that offers its automobile loans on condition that if the debtor is in arrears, the company reserves the right to prevent the debtor’s key from engaging the car’s ignition system. Although the technology is mainly deployed at the subprime level, there are still ## of interrupter starters estimated to be used in the country and the technology has presumably allowed companies to extend credit to individuals who would otherwise be deemed too risky.\(^\text{12}\)

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. For instance, a starter interrupter cannot disengage a car while it is currently running, which would have the obvious

\(^{11}\) (HF5483 .S44 2002)

potential of causing accidents. The starter interrupter can be manually overridden with a code in certain instances in certain cases where life and limb are at stake. These common sense exceptions to the power of the starter interrupters are included in many of the best practices guidelines for the industry. This would allow the companies to comply with existing law that prevents, for instance, the causing of torts on the highways.

The costs 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 increase their collection rates by locating their collateral and preventing its misuse.

Such use by creditors has drawn criticism by some who view the collection of collateral as unfair to those debtors who rely on it. Others point to the lower interest rates that can now be afforded because of the increased rates of recovery and therefore the systemically lower credit risk. This debate is beyond the scope of this article, but it suffices to say that 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 the states and so there is no federal law specifically dealing with starter interrupters. Indeed, there is not much state law on the matter. California, Colorado, and Connecticut all explicitly affirm the legality of starter interrupters, but place certain restrictions on their use. The primary concerns of the state legislatures are both

---


that the debtor has notice that the device has been installed and that the debtor has a right to cure the breach.

Instead, the use of starter interrupters is generally governed by the provisions of the Uniform Commercial Code ("UCC"), as adopted in various forms by the states, governing 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.”\(^{15}\) There is a rich case law 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.

One more area of law where there have been some judicial decisions with respect to starter interrupts has been bankruptcy cases. A bankruptcy court in Arkansas ruled that the installation of a starter interrupter, while not \textit{per se} illegal, was violative of the Bankruptcy Code’s automatic stay because it prevented the debtor from the normal use of her car. The court noted that the defendant 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.”\(^{16}\)

1. The trouble with the starter interrupter as it currently exists, however, is that it is engaged by the creditor or an agent of the creditor. Thus, to use the above terminology, the judge in the case is one of the parties who determines, given a factual pattern, which output is

\(^{15}\) U.C.C. § 9-609

most appropriate. It is a standard legal principle that no one should judge his own cause.¹⁷

Yet the starter interrupter relies precisely on this occurring. This is where we need to invoke the second technology to make the smart contract possible.

2. With respect to the Bankruptcy Code, there are a number of novel solutions that could incorporate the substantive protections of debtors and other provisions in the contractware code. It is yet to be seen whether this is devised by private actors scraping bankruptcy docket filings for certain orders by judges, the government itself providing methods of compliance, or some other method.

### The Good

#### Libertarians

- Libertarian political theory and smart contracts
  - Ameliorating the need for monopolized legal services
  - Szabo

#### Coaseans

- Lowering of transaction costs
  - Yermack work on corporate governance, security issuance, etc.

¹⁷ Nemo iudex in causa sua.
The Bad and the Ugly

Three Examples

The above has shown the benefits that come from judicial recognition and enforcement of smart contracts. Many 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. The merits of the privatized provision of justice have been commented on by many. What this section of the paper analyzes is the positive question of where the outer bound of a state’s acceptance of self-help would be.

Three examples will be helpful in demonstrating the degrees to which states and their judicial systems will recognize smart contracts.

The first example is starter interrupt devices. As was shown, courts have recognized these devices as legitimate and allowed companies to use them to repossess, provided there is no violation to the Uniform Commercial Code’s “breach of peace” provision. But what will occur when these devices violate another enforceable statutory scheme, such as the Bankruptcy Code?

Suppose a starter interrupt is placed in a truck that is essential to a part of a business. Instead of merely shutting the car off, this starter interrupt will permanently damage the car’s engine, rendering it unusable, if payments are not received on time. Then suppose a corporate debtor files for Chapter 11 bankruptcy. The debtor-in-possession or trustee could charge that the use of the starter interrupt is a violation of the automatic stay or §363 of the Code allowing for

---

18 See above.

19 Granted, the creditor is not incentivized to have his collateral destroyed, but for the purposes of this example, we will suspend our disbelief.
use of the property of the state in the ordinary course of business, as the actions are 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. The question then put to the court is whether starter interrupts can be used at all if they have such potential.

A second example further along the spectrum, would be a modern-day version of *Williams v. Walker-Thomas Furniture Co.*[^20] The court held in that case that the cross-collateralization scheme was unconscionable and that the creditor could not repossess the property. Imagine that the furniture in that case had contractware that emitted a foul odor or an annoying siren if payment was not received and that this was agreed to by the debtor *ex ante*. A court bound by *Williams*, would be bound to deem the contract unconscionable, but could it prevent the contractware from being installed with those conditions in the first place? If it could not prevent the device from being installed, then the practical remedy would be to order the creditor to pay damages. If it could prevent the device from being installed, would it simply create a new set of breaching the peace doctrines that creditors and the contractware would have to abide by.

The final example, the most egregious, would be contractware installed into humans. Although certainly a dystopian *gedankenexperiment*, it is worth imagining a nightmarish scenario where creditors can install devices into debtors and when those debtors default, have the device force them into slavery. Such a scheme would be patently unconstitutional as a violation of the Thirteenth Amendment. This is not the interesting question, however. What is worth analyzing is how a court will *ex ante* deal with such installation.

Even though there are two consenting parties, the court will find the contract a nullity. But will the court prevent the installation of the contractware into the body? This is a tougher question because it implicates an individual, *ex ante*, being able to tie himself like Ulysses to the mast.

It is hard to imagine a court condoning such contracts and it is likely that the legislature would pass a law making it illegal for an individual to tie himself to the mast in such a way.

- There is argumentation on both sides here both from a moral and legal (prospective injunctive relief) perspective

**Limiting Principles**

What the above shows 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 can the state use prior restraint to prevent the formation of contracts that have the potential to become contrary to public policy, but are not necessarily so.

The answer is likely yes. It is hard to imagine a state sitting idly by while devices are installed to self-enforce contracts that are contrary to its own interests. 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. This is the guiding principle behind the issuance of prospective injunctive relief.\(^{21}\) The Supreme Court’s First Amendment jurisprudence provides a useful model. In that realm, the Court has erred on the side of

respecting autonomy and policing *ex post*. In this instance, contractware ought not be analyzed *in toto*, but discrete devices should be evaluated. So, while devices that prevent the usage of personal property could be allowed, implants that enforce *per se* unconstitutional contracts would not be permitted.

These are questions for judges to decide through casuistry. Common law principles ought to form the background of such analysis.