Smart Contracts and the Role of Lawyers (Part 1) – About Smart Contracts

Legaltech is awash in buzz terms these days, and "smart contract" appears very near the crest of the legaltech hype wave. The reason is obvious enough: everyone knows that lawyers are the ones who draft contracts, so surely the law biz needs to pay attention when contracts get "smart." Plus, smart contracts live on blockchains, don't they? Hasn't the recent fintech interest in blockchains chummed the waters for all sorts of activities by big banks, big tech companies, government agencies, consulting firms and other well-heeled and high-paying clients of biglaw? You bet it has, and you can safely bet that lawyers are taking note! So let's check out this very fascinating but complex topic in greater depth. I've broken up my thoughts into three separate posts – this first part provides critical historical background and context for understanding what smart contracts are; the second part uses a recent notorious blockchain incident to delve into some of the interesting legal theory implications of smart contracts; and with the groundwork laid in the first two parts, the third part deconstructs the likely (and not so likely) impacts of smart contracts on transactional lawyering. These posts are lengthy and dense, but if you stick with it, I believe you will emerge with a fuller and more nuanced understanding of the hype *and* substance of smart contracts.

In the Beginning There Was the Vending Machine

Let's step back and get our bearings. Credit for the term "smart contract" is usually attributed to computer scientist, Nick Szabo, who first used the term in his 1994 article, Formalizing and Securing Relationships on Public Networks. As described by Szabo, smart contracts are a way of automating traditional (common law) contract concepts and applying them to transactions that occur primarily or

exclusively in the digital domain (ideally with no manual human intervention). Arguably, his chief insight and contribution was the outline of a formalized, potentially machine-readable language for writing and executing these so-called smart contracts. See here. Szabo used the simple vending machine as an example of how contracts can be reified in the real world and then further abstracted to the digital world:

> *The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price.* ***The vending machine is a contract with bearer:*** *anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas. Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means. Smart contracts reference that property in a dynamic, often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.*

Anyone who has sat through a contracts class in the first semester of law school will notice something amiss in the bolded text above, but before we examine that particular application of the term *contract* more closely below, let's take a brief look at how Szabo took a vending machine transaction and formally expressed it as a *smart contract*:

```
sellCandy(candyPrice = $0.90) =
    variable moneyAmount = $0.00
    then
```

```
        # coins also fall into a temporary till tempTill
    when choiceOf(Counterparty, nickel)
        to TempTill nickel
        then to Counterparty add(moneyAmount, $0.05)
        then to Counterparty display(moneyAmount)
    when choiceOf(Counterparty, dime)
        to TempTill dime
        then to Counterparty add(moneyAmount, $0.10)
        then to Counterparty display(moneyAmount)
    when choiceOf(Counterparty, quarter)
        to TempTill quarter
        then to Counterparty add(moneyAmount, $0.25)
        then to Counterparty display(moneyAmount)
    when choiceOf(Counterparty, moneyReturn)
        to Counterparty dropCoins(tempTill, returnTill)
        with moneyAmount = $0.00
        then to Counterparty display(moneyAmount)
    when threshold(moneyAmount, candyPrice)
        to Holder (nickel | dime | quarter)
            to CounterParty redirectNewCoinsTo(returnTill)
        also display("ready to dispense -- please select candy")
        then when (candySelection)
            to Counterparty dropCandy(candyRacks, candySelection)
            with to PermanentTill dropCoins(TempTill)
            with moneyAmount = $0.00
    continue
```

There you have it: a smart contract! Now, that might not seem like much of anything worth getting excited about. To be fair, a lot of what's really interesting and important in Szabo's early work relates to his conceptualizations of how cryptographic techniques could be used for the generation of digital cash and virtualizations of other forms of value and rights of parties that are common in real world commercial transactions but tricky to recreate in the digital domain. He recognized the importance of security (in both senses of the term) and noted how distributed computing strategies could be used to build a decentralized digital economy based on smart contracts. In short, much of what was eventually implemented in Bitcoin and alternative distributed ledger systems can be traced back to Szabo's insights of two decades ago.

Despite the fact that Bitcoin transactions are really just simple smart contracts (per Szabo's meaning of the term) and pretty sophisticated contract-like transactions can be modeled and executed as Bitcoin transactions, real interest in the legal sphere didn't really pick up until the Ethereum project appeared on the scene. It's easy to understand why. Bitcoin has always been used primarily as a cryptocurrency. Alt uses of Bitcoin have been generally focused on specialized applications and cryptocurrencies, and most of the private (also known as "permissioned") blockchain projects have been narrow-gauged platforms for derivatives trading and other fintech applications. See, for instance, the platforms being developed by R3, Digital Asset Holdings, Chain.com and Symbiont.io among many others. Ethereum, on the other hand, was promoted from the get-go as a public (permissionless) platform that features a general purpose programming language for constructing "smart contracts" like Szabo envisioned. In fact, the original Ethereum white paper is entitled, *A Next-Generation Smart Contract and Decentralized Application Platform.* Whether or not it was the cause or merely an effect of a growing recognition of and interest in smart contracts in the legal community, Ethereum has become the poster child for the term itself.

The Pitch is Made to Lawyers

As things stand today, smart contracts are typically introduced to lawyers in conference presentations, articles, blog posts, etc. with no real definition of what they are, what they do and where they live. At most, they are "defined" by giving specific examples such as lease agreements, loan agreements, real estate transfers and registries, trade financing and payment arrangements, IP permissioning and, of course, a variety of banking transactions and other financial services. Drawing from these real world examples already familiar to lawyers keeps things simple but also tends to downplay some of the radical breaks in how things work in the blockchain world. It also downplays the fragmented and fast-changing landscape of the blockchain world that is still full of huge "TBD" infrastructure holes with respect to contractual transactions. Most of all, an example-based approach disguises how the same kind of real world contractual transaction can be (partially) modeled in fundamentally different ways on a blockchain, with very different legal implications and completely different impacts on the role of lawyers in the (smart) contract creation and execution.

The problem originates from the incomplete nature of a *smart contract* as the term was originally used by Szabo. Getting back to our law school contracts class concern, the vending machine in Szabo's proto-smart contract example only explicitly models the *performance* stage of a contract. The *form and formation* stage is mostly just implied and assumed by our prior knowledge and experience with these machines, and thus, the term is infused with more conceptual weightiness than it really deserves. Would any lawyer ever characterize an unmarked black box with a slot at one end and a hole at the other as a "contract" knowing nothing else about it? No, of course not. What fundamentally differentiates a soda machine from an automobile is the implicit presence of the *legal concept* of a "meeting of minds" associated with the insertion of a coin in the coin slot but not with the insertion of a key in the ignition slot. Clearly, what makes a contract uniquely a contract and not some other form of interpersonal or automated activity is largely frontloaded in the form and formation stage of a contract and must be taken as an *a priori* condition in any deterministic form of human/machine interaction.

This problem with smart contracts has not gone unnoticed. Ian Grigg, for instance, describes it as a "semantic" weakness of smart contracts. His "Ricardian contract" proposes a way to model the contract form and formation stage online by specifying methods for tamper-proof recordation and validation of human-readable/natural language contracts with provable assent by the parties involved. Others, like the CommonAccord project, also focus on the form and formation stage with an emphasis on templatization and formalization of the contract terms. All of these contract form/formation efforts have jumped onboard the blockchain train, recognizing that this relatively new technology represents an increasingly legitimized business platform for hosting contracts/contract artifacts online in a reassuringly neutral and secure way. Not surprisingly, these form/formation efforts tend to be much more lawyer-friendly and lawyer-led because they generally leverage familiar legal concepts and protocols. By contrast, smart contract work has been done primarily by computer programmers based on leveraging concepts from computer science, cryptography and game theory.

The potential benefits of blockchain-based recordation of contracts should not be underestimated, just as the potential for automated contract performance via

smart contracts is huge. However, as long as efforts to model contract formation and performance remain disconnected from each other, the broader issue of how blockchain-based transactions (including the numerous examples noted above) are to be interpreted and treated legally remains unresolved. Eris Industries was an early proponent of integrating the recordation of legal prose with the execution of smart contracts. R3, which is now touting the ability of its Corda platform to holistically capture legal prose and executable smart contracts, appears to recognize the value of supporting a more rigorous analysis of blockchain-based contracting. The success of these efforts remains to be determined, but it seems likely that the role to be played by lawyers and law firms in this new environment will be closely tied to how well drafting, formation and recordation processes (the traditional purview of lawyers) are integrated on-chain with the automated/smart execution processes (the programmers' purview).

Up Next

Before we explore the lawyering impact further in part 3 of this series of posts, we need to dig a little deeper into another dimension of smart contracts not touched on above. It starts with a riddle that should be of considerable interest to lawyers: *When is a $60 million breach of contract not a breach?* For the answer, check out my next post...

Related

Smart Contracts and the Role of Lawyers (Part 2) - About "Code is Law"

October 22, 2016
In "Smart Contracts"

Smart Contracts and the Role of Lawyers (Part 3) - About Lawyering Transactions on Blockchains

October 25, 2016
In "Smart Contracts"

Dabbling

February 9, 2016
Similar post

Brent Miller / October 20, 2016 / Smart Contracts

6 thoughts on "Smart Contracts and the Role of Lawyers (Part 1) – About Smart Contracts"

Sally Wheeler

October 23, 2016 at 11:10 am

This is very interesting indeed – the only thing that I have read on the contract law angle of this.

Chris Cook

October 23, 2016 at 2:52 pm

This article on Fintech 2.0 might be of interest on this subject

https://blog.p2pfoundation.net/fintech-2-0/2016/10/06

In a nutshell, absolute/digital Property rights & instruments do not interact well with an analogue world

Brent Miller

October 23, 2016 at 6:17 pm

Thanks for the link to your interesting article. Regarding your "nutshell" statement, I would argue that "property rights" is an analog concept. The trouble begins when we try to apply analog concepts to the digital domain. Things get real messy real fast, as is illustrated by "The DAO" disaster I discuss in my Part 2 blog post. Check it out.

Chris Cook

October 23, 2016 at 7:02 pm

Nice article re the DAO – a colossal mess which I have to say kept me laughing for a couple of weeks and I am still chuckling about.

It is said that there are as many Sumo wrestlers in the US as there are attorneys in Japan, and my experience is that the Japanese will achieve in a couple of pages what takes us forty or fifty, because trust is assumed and they are not trying to think of every which way the other guy can screw them.

There are other traditions East of Suez in Sharia'h, India and China but the bottom line is that our 'Anglo' Rule of Law tradition with roots as far back as the Greeks has never really caught on. But just to be contrarian, here in Scotland we have three verdicts in a criminal case: Guilty; Not Guilty & Not Proven.

The first two represent either/or absolutes: 'Not Proven' is the legal equivalent of a Platypus. These absolutes are reflected in terms of Property rights by absolute (Divine Right of Capital) ownership of infinite duration on the one hand eg Freehold land and Joint Stock Shares – and the absolute/finite (for a term certain) duration of Leasehold and Debt. So when I speak of digital property rights I am referring to the conflicting absolute claims over potentially the same productive asset.

But there is another (third) non-Absolute approach which is a right with indeterminate/ indefinite duration. An example is a generally acceptable credit

instrument – aka currency – which is a promise returnable in payment for value to be supplied by the promissor. There are other examples such as overdrafts, tenancy at will and so on.

My work concerns associative/interactive agreements and protocols – clubs, if you like – which may be both open AND closed; Private AND Public. A Club of (say) car users is closed, becaus eonly members may use the cars, but also be open since anyone who agrees to the rules & standards may join.

I was a member of a Housing Co-operative in London for 10 years and my (indefinite) right of occupation was not freehold; or leasehold or even as a tenant. It arose through membership of a UK Corporate entity known as a Friendly Society.

It is here – in what the French term associative 'contrats de societe' to distinguish them from our statute and judge-made 'contrats de mandat' – that I believe that law meets code, and suitable consensual agreements may be combined with simple promises/credit instruments to enable a networked political economy bottom up.

The reason why I think this is inevitable is that these consensual protocols and 'open' instruments are not new – they actually pre-date what we have created since – and they are both complementary to our fundamentally broken system and capable of out-competing them because of the absence of 'something for nothing' aka economic rent.

I have even come up with a term to describe the necessary 'platform co-operative' agreements – Nondominium – where no stakeholder has a dominant right to impose on any other, but all have rights of veto and simply walking away.

https://blogs.ucl.ac.uk/resilience/2013/01/16/submission-by-chris-cook-to-the-land-reform-review-group/

Brent Miller

October 23, 2016 at 8:21 pm

Your reference to the tradition of trust in Japanese lawyering made me realize the irony that the nom de plume of the "inventor" of trustless blockchains is "Satoshi Nakamoto." 😉 Alas, those corrupting western influences have caused the number of Japanese-qualified lawyers to skyrocket (to say nothing of the number of non-qualified western lawyers working in Japan). I find your exploration of alternative conceptions of property rights made possible by technological developments to be a really fascinating and interesting one (but not one in which I have any personal expertise). Thanks for making the connection for me. I hope to dig into it some more. My prior interest in "code is law" touches on a related problem of what happens when we attempt to model in the purely digital domain legal concepts that are nominally binary but almost never rigorously so in application. How does one mathematically express "Guilty" and "Not Guilty" let alone, "Not Proven"?!?

Pingback: Smart Contracts and the Role of Lawyers (Part 3) – About Lawyering Transactions on Blockchains – Biglaw KM

Comments are closed.