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

In my previous post I described how "smart contracts" are not really contracts in the comprehensive or strict sense of the term as understood and used by lawyers. Smart contracts only explicitly model the performance aspect of a real world contract and implicitly assume the form and formation aspects of a contract. If we simply admitted the term, "smart contract" is an unfortunate historical accident and relabeled it to something like "chaincode" or just "script" as some platforms refer to it, then a lot of the conceptual baggage and terminological confusion would probably disappear. Of course, a lot of the sexiness of the term and apparent relevance to lawyers might disappear as well. Nevertheless, the expanding interest in blockchain-based transactions by financial institutions, exchanges, other businesses and governmental agencies seems like fertile ground for lawyers to plow, regardless of how the particulars are labeled. Or is it a quagmire instead? The answer is not a simple one to give as is well illustrated by the recent failure of what is probably the single largest blockchain-based smart contract ever created.

The $60 Million Bug That Was Also a Feature

Our story begins with the launch of "The DAO" (TheDAO), an ambitious project to create the first large-scale distributed autonomous organization on the Ethereum smart contract blockchain. TheDAO was intended to automate crowdfunding of submitted project proposals from a collected pool of "Ether" (the Ethereum cryptocurrency that is exchangable with Bitcoins, US Dollars or other fiat currencies). All governance and funding decisions were based on proportional participant voting without further human intervention (except for one special case not relevant here). As explained in TheDAO wiki:

> *[TheDAO] is represented by smart contracts on the Ethereum Blockchain. It contains functions which, as a whole, have analogies to a crowdfunding vehicle governed by participants' votes, to seek out and fund proposals. Because [TheDAO] consists of computer code, it interacts with the physical world through Contractors. The creators of these proposals act similar to a contractor, with [TheDAO] as its client. [TheDAO] therefore does not "invest" in these proposals, because it does not acquire equity in the contractors. Instead, in return for receiving a funding by [TheDAO], contractors deliver services, infrastructures or products yielding a return to [TheDAO].*

TheDAO was wildly successful in raising funds. In the single month of May, over 10,000 participants contributed Ether equal to over $160 million USD, and project funding proposals started rolling in. While some experts raised alarms about the code itself, questioned the validity of TheDAO as a legal entity, worried that the launch represented the sale of unregistered securities or imposed general partner liability for TheDAO participants, others praised the project and called it a revolutionary leap forward. It didn't take long for disaster to strike…

In mid June, one of TheDAO participants exploited a vulnerability built into a particular withdrawal function in TheDAO's smart contract and seized control of approximately one third of its Ether-based assets (worth about $60 million USD). Restrictions coded into the smart contract locked up the drained Ether for a specified period of time (about a month) and prevented a completely irreversible and potentially untraceable withdrawal by the participant/attacker during the lock-up period. Likewise, other coded restrictions prevented other "white hat" participants from fully retrieving the Ether as well. Stalemate? Not quite. Influential members of the Ethereum community initially proposed a solution known as a "soft fork" that requested all of those involved in operating (a/k/a "mining") the peer-to-peer network of servers that constitute the Ethereum blockchain to, in effect, ignore the problematic transaction and treat all subsequent transactions on the blockchain as if it never happened. This rewriting-of-history proposal was withdrawn after further testing revealed that the soft fork was vulnerable to hacks. In it's place a "hard fork" solution was proposed that required participating miners to change the software they used to maintain the blockchain.

Approximately 85% of the Ethereum miners adopted the hard fork, but because the remaining miners pledged to continue with the old code, Ethereum split into parallel crypto universes, identical in most respects with identical account balances and account holders of Ether (designated as ETH in one and ETC in the other) with one critical difference: the hard-forked Ethereum universe essentially treated TheDAO’s smart contract as rescindable by all participants due to mutual mistake, and the non-forked Ethereum universe continued to treat the attack as a valid transaction within the terms of TheDAO’s smart contract. In the former instance, TheDAO participants were placed in a position to recover the Ether (ETH) they owned just prior to the June attack. In the latter instance, the attacker continued to control a large amount of Ether (ETC) at the expense of the rest of TheDAO participants.

Having trouble following this? Here’s an analogy that might make more sense to lawyers: A soft drink company is reorganized into two separate entities in an effort to fend off a hostile and (some would argue) illegal takeover by an insurgent shareholder. Both of the successor companies get rights to the magic soft drink formula, but one receives 85% of the bottling facilities and distribution capacity and the other receives the remaining 15%. Through some questionable changes in the original company’s bylaws proposed by the company’s lawyers and adopted by the board of directors, the original shareholders are issued stock in the larger successor in proportion to their ownership prior to the attempted hostile takeover and issued stock in the smaller successor in proportion to ownership of-record as of the reorganization date. These changes leave the insurgent shareholder with a tiny stake in the larger successor and a big stake in the smaller successor. When shares in the new companies start trading on exchanges, the price of shares in the larger successor is bolstered by the extra assets and perception of market domination but tempered somewhat by residual concerns surrounding the dubious corporate governance manipulations. The opposite applies to the value of shares in the smaller successor. Thus, depending on whether you are a shareholding executive of the original company, the insurgent shareholder, an institutional shareholder, a speculative trader or just an individual with a few shares, you might be relieved, indifferent or outraged and considering legal action.

In the physical world as governed by the sovereignty of laws, regulations and courts (hereinafter, "real space"), the process for determining the validity of the corporate actions taken to repel a hostile takeover like the dubious one described above is well understood. Likewise, the advisory and advocacy roles of lawyers in that process is well established and critical. Lawyers are the tour guides through the sovereign institutions in which real space contracts are formed, executed, performed and adjudicated when disputes arise. All well and good, but what about the virtual world of "cyberspace" in which things like DAOs and smart contracts exist? When smart contracts go awry as happened with TheDAO, isn't there an important role for lawyers to play in resolving the issues? Isn't there also an important role for lawyers to play in preventing those problems from arising in the first place? Not surprisingly, an increasing number of lawyers have stepped forward to answer in the affirmative. See, for instance, here.

The affirmative answer that lawyers (and not just programmers) need to be involved in smart contract preparation makes sense and works well only when talking about one kind of blockchain-based decentralized cyberspace (the kind that banks are playing with). It does not work so well when applied to the kind of cyberspace that many envision Ethereum to be. This is important! *Structural differences between permissioned/consortium blockchains like the ones favored by banks vs. permissionless/public platforms like Bitcoin and Ethereum reflect two dramatically different visions ("ideologies" even) at play here. The meaning and function of smart contracts and the role of lawyers with respect to them will vary dramatically depending on which vision is applied.* The remainder of this post outlines these competing visions and sets the stage for further discussion in my next post on the implications for lawyering in the brave new cyberspace(s) of blockchains.

Code is [Not] Law

As noted in my prior post, Nick Szabo showed how *[computer]* ***code is contract*** (albeit only partially so as I explained). Lawrence Lessig in his book *Code* is credited with showing how *[computer]* ***code is law****:*

> *In real space, we recognize how laws regulate – through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates*

> *– how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law." "Lex Informatica," as Joel Reidenberg first put it, or better, "code is law."* L. Lessig, *Code 2.0*, at 5.

Taken together, these two powerful concepts define how privately created transactions like smart contracts become their own private sovereignty in cyberspace, but also one that Lessig insisted should not be immune to public constraints of laws, economics and social norms:

> *[Contract rights and obligations in cyberspace] are not conditioned by the public values that contract law embraces. Its obligations instead flow automatically from the structures imposed in the code. These structures serve the private ends of the code writer; they are a private version of contract law. But as the Legal Realists spent a generation teaching, and as we seem so keen to forget: contract law is public law. "Private public law" is oxymoronic…To the extent that these code structures displace values of public law, public law has a reason to intervene to restore these public values.* L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, at 530.

Thus, for Lessig the term "code is law" acknowledges the deterministic nature of smart contract performance/execution, but not its finality. This "weak" version of the term "code is law" permits a communal ("public law") override of explicit but "buggy" code like the withdrawal function in TheDAO smart contract. It follows that the equitable recission solution generated by the hard fork adopted by 85% of the Ethereum miners was the right course of action and consistent with what Lessig meant by "code is law."

However, when Lessig wrote *Code*, cyberspace was not so isolated from real space and much of his attention was focused on the interplay between the two spaces and the continuing power of state authorities over cyberspace. Things have changed considerably in the "architecture" of cyberspace since Lessig first wrote about it at the turn of the century. In effect, cyberspace has become more anarchic and resistant to the reach of sovereign authorities. The emergence of decentralization, censorship resistance and trustless interaction on Bitcoin and

other public blockchain platforms like Ethereum has resulted in a reinterpretation of "code is law" by many blockchain enthusiasts:

> *For the first time in history, citizens can now reach consensus and coordination at global level through cryptographically verified peer-to-peer procedures, without the intermediation of a third party. The blockchain technology ushers in a new era of decentralization on large-scale, in which human factor is minimized and trust shifts from the human agents of a central organization to an open source code. In such distributed architecture, "code is law": the protocol is open-source and it can be reviewed by anyone; the network is not owned nor controlled by any single entity; data are simultaneously kept by all nodes, thus ensuring proper redundancy. Neutrality of the code, distributed consensus and auditability of transactions can significantly reduce or overcome frictions and failures inherent in decision-making process of centralized organizations (e.g. lack of transparency, corruption, coercion, etc.). Many new decentralized governance models and services can therefore be implemented and experienced through the blockchain,* ***without the oversight of governments.*** From *Blockchain. Blueprint For a New Economy*, by Melanie Swan, as quoted in M. Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, at 7 [emphasis added].

In other words, the resiliency of peer-to-peer networks, the normative power of game theory and the cloak of pseudonymity, all wrapped in high levels of cryptographic certainty, make it possible to sever most (if not all) of the lingering regulating power of real space authorities over cyberspace participants. The *Lex Informatica* of Lessig's cyberspace era gives way to the alegality or *Lex Cryptographia* of the blockchain era:

> *The advent of Lex Cryptographia may force us to reevaluate the interaction between these regulatory levers [laws, norms, economics and architecture]. One of the key consequences of the blockchain could be a rapid expansion of what Lawrence Lessig referred to as "architecture"—the code, hardware, and structures that constrain how we behave—or at a minimum a redefinition of how laws and regulations are designed, implemented, and enforced.* A. Wright & P. De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* at 50.

To the true believers of public blockchain technology, the ascendancy of this new cyberspace "architecture" means that "code is law" can now be read quite literally and with finality. They see DAOs and other smart contracts transacted on public blockchains as self-defining, self-regulating and immune from ordinary legal processes. It follows that a strict "code is law" reading of TheDAO's smart contract permitted the so-called attacker to utilize the withdrawal "feature" to drain assets contributed by other participants. To these true believers, the Ethereum miners who stayed the course of the original blockchain protocol were righteous defenders of the sovereignty and integrity of the Ethereum cyberspace. As for the other participants in TheDAO…well, any losses they suffered were caused by their own inadequate reading/testing of the smart contract and failure to heed the warnings of those who predicted problems. That is what "code is law" now means to this audience. Ironically, the term has drifted so far from Lessig's original meaning that "code is NOT law" is becoming the rallying cry for those who argue along the same lines advanced by Lessig when he originally wrote that "code is law."

The Schism

As I see it, these diametrically opposed interpretations of "code is law" reflect the deep schism that exists between two blockchain technology camps: the "crypto-purists" and the "crypto-pragmatists," as I'll label them. Both camps are simply talking past each other due to their conflicting assumptions about the purpose and core architecture of blockchain-enabled cyberspace and the function of smart contracts within them.

The Crypto-Purists. Let's start with the strict interpreters of "code is law" (e.g., the Ethereum "classic" proponents who opposed any extraordinary efforts to rescue TheDAO). For these crypto-purists (or "crypto anarchists" as some refer to them), the perfect cyberspace is characterized by total independence from all state-based authorities and their coercive regulatory activity. Crypto-purists seek to achieve a complete break by means of decentralization of governance based on trustless, self-interested behavior among participants in the space. Maximizing pseudonymity of participants (including miners) minimizes the risk of interference by state authorities and manipulations by other participants. The

public (permissionless) blockchains like Bitcoin and Ethereum come closest to achieving this ideal, but none of them fully realize the ideal (yet) for various technical and practical reasons. Crypto-purists tend to distrust and avoid real space authorities and regulation even when they might be helpful (e.g., formation/registration of TheDAO as a legal entity). Likewise, crypto-purist norms are spawned from what works best under ideal conditions of a fully decentralized and alegal cyberspace. In this mode of thinking, real space legal conventions of "intent," "fairness," "reasonableness," "equity," etc. have no long-term usefulness and are tolerated, if at all, only as a temporary crutch until the architecture of the space is fully implemented. Use of such terms to rationalize fixes like TheDAO hard fork is not countenanced.

The Crypto-Pragmatists. This "code is NOT law" contingent is driven by pragmatic considerations of how to utilize blockchain technologies to address real space inefficiencies. Crypto-pragmatists embrace – or at least accept – laws and regulations as necessary conditions or benefits of working within real space sovereignties. With that in mind, confirmable identity of blockchain participants and transparent access by state authorities to immutable on-chain transactions are viewed as conditions for protection against collusion, fraud, hacks and other destructive/anti-social behavior that can never be fully solvable by (computer) code alone. Crypto-pragmatists generally prefer permissioned/consortium blockchain platforms, partly because they circumvent some of the algorithmic inefficiencies associated with public/permissionless blockchains like Bitcoin and Ethereum, and partly because they do not scare away real space institutions like banks. For crpyto-pragmatists, *computer* code is parol evidence, *not* law, because smart contract transactions are ultimately subject to judicial/arbitral review governed by applicable legal prose and real space laws. Thus, pairing human readable legal prose with smart contracts is critical for *fully forming a real contract* that captures intent, establishes mutual assent and provides direction for resolving disputes. From the crypto-pragmatist perspective, TheDAO was fatally deficient from the get-go because it was not a fully formed and enforceable contract and its pseudonymous structuring invited attacks. These deficiencies led to disaster and forced the Ethereum community to take drastic, confidence-shaking measures

in pursuit of an equitable on-chain solution in lieu of more appropriate options for enforcement of remedies (or even criminal sanctions) off-chain.

Lawyers to the Rescue?

As already noted, no lawyers (as far as I can ascertain) were involved in the planning and coding of TheDAO. The sole legal step taken was to set up of a Swiss SARL company (DAO.Link) as a real space intermediary between TheDAO and contractors. TheDAO project raised a very large amount of capital and initiated operations with virtually no lawyer fees, accountant fees, regulatory filing fees, taxes, administrative overhead, and no associated time delays. From the crypto-purist perspective, the actions of TheDAO organizers to skip virtually all traditional lawyering and related activities was perfectly rational (and extraordinarily efficient). The problem was inadequate computer coding, not inadequate lawyering. From the crypto-pragmatist perspective, traditional lawyering might have avoided the disaster by incorporating legal prose (to establish the legal intent of the withdrawal function) and basic KYC/accreditation procedures (to identify the participants, including the eventual attacker). It might have...but it also might have made the project financially unviable, unmarketable and untimely.

As TheDAO story nicely illustrates, the relevance and value of lawyers to the production of smart contracts and the support of blockchain technology is far from obvious. It will depend, of course, on the overall progress and adoption of blockchain technology but also on the relative success of projects based on the two competing approaches. Grand pronouncements and sweeping predictions that fail to account for the differences are suspect. Proceed with caution! (But proceed anyway to my next post on how smart contracts will affect different aspects of transactional lawyering.)

Related

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

October 20, 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 22, 2016 / Smart Contracts

1 thought on “Smart Contracts and the Role of Lawyers (Part 2) – About “Code is Law””

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

Comments are closed.

Biglaw KM / Proudly powered by WordPress