Title
Ledgers and Law in the Blockchain

Authors
Maurer, WM
DuPont, QI

Publication Date
2015-06-23

Peer reviewed

Ledgers and Law in the Blockchain

Quinn DuPont and Bill Maurer — Jun 23rd, 2015

Most of the talk about Bitcoin has centered on its potential as a new form of currency, or on the use of the underlying technology as a new electronic value transfer platform or protocol. At the payments industry conference Money20/20 in the autumn of 2013, Bitcoin promoters were declaring that Bitcoin was "like SMTP [an email protocol] for money." It promised a universal protocol allowing different existing payments providers to transfer value using the Bitcoin blockchain to any other endpoint. At the same conference, Bitcoin advocates were stickering the exhibit hall, posting hand-written signs, and passing out leaflets and magazines. By 2014, however, the promise of the protocol seemed to have come to fruition: Bitcoin-based payment providers like BitPay and Coinbase purchased elaborate booths for Money20/20, and had developed professional collateral to advertise their services—and, perhaps more importantly, showed their desire for legitimacy and market dominance alongside traditional payment providers, such as Western Union, Visa, or PayPal.

About this same time, however, there were ripples (so to speak) in the Bitcoin universe. New, non-Bitcoin based startups launched, each a little different in terms of the underlying technology and promise. A new company called Ripple put itself forward as an electronic settlement infrastructure, based on distributed consensus in a communications network rather than a distributed blockchain database. It would go on to operate almost like an interbank clearing service, until it was fined by the Financial Crimes Enforcement Network (FinCEN) of the US Department of Treasury for operating as an unlicensed money transmitter.[i] Ripple inherits the ledger technology from Bitcoin but utilizes a network of

trusted parties ("validation" nodes), much like the way traditional financial services operate, instead of the computationally expensive and slower mining system of Bitcoin. Additionally, while Bitcoin is a system of currency, Ripple is a system that transfers debt obligations, not money. Other start-ups, Ethereum and Eris, each offered distributed, blockchain-based systems for creating and running applications without a central server or authority as a control point. These services promise a way to use the core qualities of blockchain databases to craft peer-to-peer applications that can be autonomous and self-executing. Ethereum and Eris also inherit the blockchain technology from Bitcoin but generalize its use beyond the exchange of currency, putting software code, not transaction data, on the blockchain. Unlike traditional software running on a single computer, Ethereum and Eris are, in a way, "cloud" service providers—but they avoid the centralization implicit in traditional cloud service providers. Unlike, say, using Amazon servers to host your software, these services are decentralized among peers so that no one peer (or company) can stop service or act maliciously. One of their primary use targets is the so-called smart contract, a (decentralized) piece of software capable of enacting legal contracts autonomously, an idea first proposed by Nick Szabo in 1997. Blockchains, it seemed, were moving from the money space to the law space.

The blockchain, the ledger and the contract

The core qualities new enterprises like Ethereum exploit all have to do with underlying features of blockchains as records-keeping devices, and peculiar ones, at that. A blockchain is a database or ledger that is distributed among all the nodes in the network running it (at least in theory). Each node has a complete copy of the entire database (again, at least in theory). Modifications to the database have to be verified by enough of the other nodes to warrant that modification's validity. Bitcoin uses a lottery-like proof of work system to effect this, but other systems can do it differently. Regardless, the key characteristics of a blockchain that make it a special kind of ledger and that are particularly appealing to developers and proponents are that it is: distributed, decentralized, public or transparent, time-stamped, persistent, and verifiable.[ii]

Developers using services like Ethereum want to use these characteristics of blockchains to create distributed autonomous organizations that can do different kinds of work without the intercession of intermediaries, central authorities, the state, the dominance of one individual, or a controlling junta. The decentralized, distributed character of the thing makes that impossible (so long as the system remains fully decentralized, since in practical terms such systems are still subject to collusion). The publicity, verifiability and time-stamped features make the thing trustworthy to all peers in the system, who rely on their own contributions to the maintenance and verification of the blockchain to warrant its truth. Its relative permanence or persistence makes it a new kind of authoritative record without any central, overarching authority.

That seems to be an awful lot of work for a ledger to do. Or is it? Blockchain systems occasion a reconsideration of two of the central legal devices of modernity: the ledger and the contract. There is a vast historiography on the role of accounting in the rise of capitalism and modernity. There is an even larger archive of history, jurisprudence and philosophy of the

contract. Indeed, the contract has long been considered as foundational to the Enlightenment as well as incipient to ancient Greek thought. We know of such systems today because they have persisted in material form, and have developed into long-standing bureaucratic apparatuses. The ledger and the contract have worked in tandem to structure and interpellate human relationships, creating "Man" [sic] itself. These apparatuses become powerful *because* they have been placed in certain social contexts, negotiations of social context that get inscribed within ledgers and contracts. For all the hype surrounding the blockchain as a replacement for these essential apparatuses, the blockchain actually occupies an old role. Indeed, one could argue that the degree to which blockchains will succeed in materially replacing the ledger and contract is correlate to the degree to which it hews closely to these ancient functions.

We are not going to review the vast literatures about the origins of modernity. Instead, looking at selections from the histories of accounting and contract technologies allow us to reflect on what blockchain systems might do—what they might already be doing!—to these cornerstones of the modern era.

Our examples are not quite chosen at random. Let's dive in.

1. Look at Moore's Modern Methods:

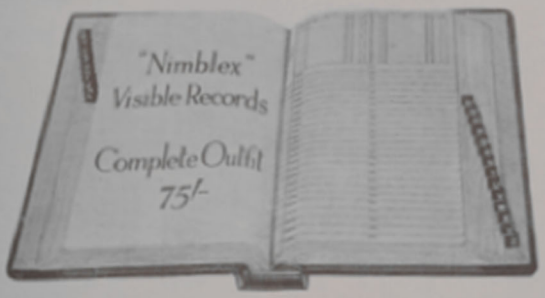
Moore's Visible Loose-Leaf Books

BRITISH MADE

THE "NIMBLEX"

(Registered Trade Mark No. 474500.)

VISIBLE Record-keeping affords so many advantages over "blind" systems that it is growing more and more popular every day, particularly where speedier reference is wanted.



Until the introduction of the "Nimblex," the cost of equipment militated against the general use of "Visible" Records. But now "Nimblex" meets the demand for an inexpensive visible method, suitable for both large and small businesses, and the receipt of an increasing volume of repeat orders testifies to its efficiency.

The "Nimblex" provides all the facilities for quick reference afforded by the more costly Visible Card Systems, and it occupies but an eighth of the space.

Full particulars of the "Nimblex" are given in Section 4. See also page 46.

NIMBLEX
MOORE'S
VISIBLE RECORDS
BRITISH MADE

The Visible Loose-leaf Book without the hump.

See page 140.

Moore's Modern Methods was founded in 1909 as a manufacturer of filing and binder supplies for governments and businesses (it has since become Moores of London, retaining the binder tradition in custom made leather portfolios and the like). Maurer first

encountered it during his fieldwork in the British Virgin Islands. Regular ruled ledger sheets made by Moore's Modern Methods (hereafter, MMM) had replaced handwritten and typed property deeds there in the 1970s.[iii] The effect of this transition to the MMM's ledger was to cut off room for maneuver in land disputes. Where prosaic long-form descriptions of property boundaries or claims left much open to interpretation, MMM's ledger forced everything into standardized rows and columns.

Take a look at MMM's Nimblex System. The reference to "visible" record-keeping may sound strange to our ears, but in the early 20th century it referred to newfangled card and paper devices that make it possible to see at a glance a great deal of data at once, to provide, as the ad for Acme Visible Records puts it, "'fact-power' control!" So-called blind systems, in contrast, would have been stacked or stapled sales receipts kept in boxes or card-catalog type systems, hiding that data away.

MMM's systems made things visible. They also helped structure decisions. They controlled workflow and thus structured bureaucratic processes. They also provided a visible time-stamped record of transactions, which could be cross-referenced for verifiability.

Although they were "visible," these technologies were private—that is, they were not open to just anyone, but only to proprietors, managers, accountants or employees. Their visibility, however, meant that audit was easy, and they could be made public in case of disputes: disputes like breach of contract, failure to deliver, failure to pay by a specified time, and so forth. Those contracts are "outside" the ledgers—they require different pieces of paper, different authors and intermediaries, lawyers and the like. But their efficacy depends on what is going on inside those ledgers. The ledgers did not embed recourse in themselves, as Ethereum seems to be trying to do (or perhaps eliminate altogether, since Ethereum contracts execute their terms automatically), but could be used if legal recourse was sought. That is to say, if something were to go wrong—if there were a dispute, or a legal claim—one could bring the visible records out into the open and put them into evidence before a court or other third party. The remedy to a problem is, like the contract, *outside* of the ledger technology. Ethereum seems to build the contract and the remedy in case of its breach *inside* the technology, as we will discuss below.[iv]

The very earliest ledgers were stored alongside other private and precious things, even in an actual room or closet that was accessible only by the male head of the household and his most trusted (male) confidants (there is some suggestion that the phrase "coming out of the closet" arises from this context). Because the double-entry ledger was the most public part of the accounting system it substituted its prescribed, facing-page, double system of recording transactions for the literal security of more private books, such as the daybook or journal stored in a locked room or safe. According to Mary Poovey, it was only by publishing the *rules* of the system of accounting that people would come to believe it accurately reflected the financial reality. Printing accounting manuals promoted an internally consistent, reliable standard.

The publication of accounting manuals transported the system of management from the private closet to a public space, and in so doing became a critical apparatus for business and helped create modernity itself. In the early days of the development of double-entry ledger systems their publication became a vehicle for promoting emerging mercantile power against the King's traditional rule. Poovey argues that the social function of double-entry bookkeeping, as an "apologist for mercantile honesty" (37), coincided with the appearance of printed books about it. Such accounting manuals prescribed order to accounts by prominently depicting balances on facing pages, for every credit on the one page there is a corresponding debit on the other. The ledgers were internally accurate according to prescribed rules, but their interface with the outside world was created whole cloth to ensure that the ledgers would balance. Interaction with the outside world necessitated creating balance in a way that might seem, from the outside, erroneous or even fraudulent. The ledgers substituted formal precision for accuracy to the external world. A consequence of this fabrication is that it was difficult to actually determine financial standing. We might accuse the system of being ethically bankrupt, but such an accusation is to buy into the form of precision promulgated by the system itself, then turn it back on to itself from the outside, and expect or demand it to entertain such realities. This is a category mistake: expecting the internal order of the books to actually occur in the flesh and blood world is to put the cart before the horse. In the melee of business, visually ordered accounts *suggested* an orderly

world, making believe that the honesty and virtue of business was as plain and transparent to anyone who cared to inspect the ledger.

Modern systems like the Nimblex also came with manuals. MMM's 1934 catalog lists 19 instructional publications, with titles like "Selling Costs and Records," and leaflets, such as:

***Leaflet No. 125**—a full explanation of the **Duplicate Statement System** for the use of traders who render detailed accounts to their customers, weekly, monthly, or quarterly. A real time saver.*

Ledgers existed in a *system* of books, producing social effects that exceeded transcription and calculation. Taken together, these books established a mode of government, which William Petty (1623- 1687) called "political arithmetic." Petty's political arithmetic was based on the surety of "number, weight, and method" so as to compel assent to the system. The simple mathematics used in the ledger transformed abstract representations into usable facts for governance.

2. The Compte Rendu:

REVENUS

PORTÉS AU TRÉSOR ROYAL.

		l.	l.
1.	Recettes générales des finances des pays d'élections		119,540,000
2.	Fermes générales unies		48,427,000
3.	Droit du domaine d'occident, régi par la ferme générale		4,100,000
4.	Régie générale		8,903,000
5.	Domaines et bois		38,100,000
6.	Postes et messageries		9,012,000
7.	Impositions de la ville de Paris		5,745,000
8.	Poudres et salpêtres		800,000
9.	Dixième d'amortissement, et anciens dixièmes retenus par les trésoriers		1,182,000
10.	Revenus casuels, compris les jurandes		3,928,000
	PAYS D'ÉTATS, déduction faite des intérêts d'emprunt et des capitaux employés en remboursement, etc.		
11.	Bretagne. du trésorier des états... 4,573,000 ; du receveur général des finances... 66,000	4,639,000	
12.	Languedoc. du trésorier des états... 946,000 ; du receveur général des finances.. 386,000	1,332,000	
13.	Bourgogne. du trésorier des états..	48,000	
14.	Bresse, Bugey et Gex. du receveur général des finances..	458,000	
15.	Provence.. du trésorier des états..	574,000	
16.	Terres adjacentes de Provence.... du receveur général des finances....	741,000	
17.	Navarre et Béarn. des receveurs généraux des finances..	323,000	
18.	Pays de Foix.... du receveur général des finances.....	100,000	
			8,215,000
			247,952,000

		l.
	Report	247,952,000
19.	Recette des finances du Roussillon	338,000
20.	Don gratuit du clergé, supposé de 16 à 18 millions tous les cinq ans	3,400,000
21.	Monnoies du royaume	500,000
22.	Ferme de Sceaux et de Poissy	350,000
23.	Part du roi dans les produits qui excéderont les sommes fixées pour la ferme générale, pour la régie générale et pour la régie des domaines	1,200,000
24.	Augmentations sur tous les vingtièmes abonnés	990,000
25.	Loterie royale de France et petites loteries	7,000,000
26.	Extinctions, dans l'année 1781 seulement, de rentes viagères et d'intérêts de capitaux éteints par des remboursemens	1,850,000
27.	Contributions de la ville de Paris dans les dépenses des carrières, de la garde et de la police, que l'on verse actuellement au trésor royal, attendu que le trésor royal s'est chargé de la totalité de ces dépenses	204,000
28.	Capitation de l'ordre de Malte	40,000
29.	Affinages de Trévoux, fiacres de provinces, etc.	40,000
30.	Intérêts d'environ six millions d'effets publics rentrés au trésor royal en différens temps, et non encore brûlés	290,000
31.	Rentrées de débets ou de vieilles créances et autres petites recettes imprévues. *Mémoire.*	
		264,154,000

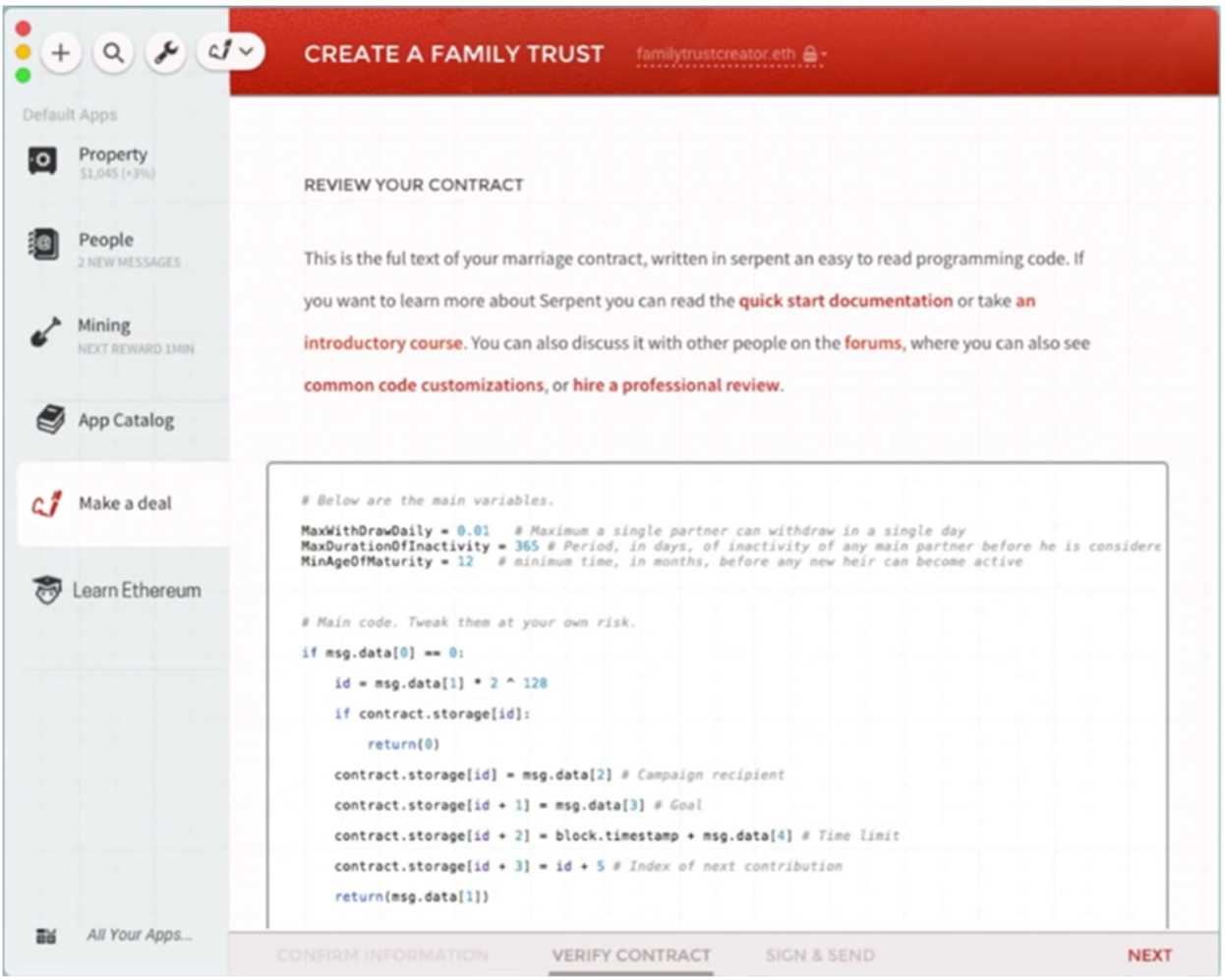
Nota. Le surplus des revenus du roi est employé à payer les dépenses assignées sur différentes caisses.

The Compte Rendu was an accounting of all the expenditures of the French state created just prior to the Revolution. Published in 1781 by the minister of finance, Jacques Necker, it presented a rosy picture of the state of French public finance. This strengthened the position of the King, as well as Necker's own political fortunes. The Compte Rendu produced, in double-entry fashion, all of the revenues and expenditures of the royal house. According to Jacob Soll, this both demystified the sovereign, rendering it a "shocking set of numbers" (140), and also allowed Necker to launch a careful critique: although his figures showed an overall budget surplus, it also revealed exactly how much the royal house was spending on frivolous things. Soll shows how it thereby sowed seeds of revolution.

The Compte Rendu became a best seller, selling 100,000 copies in 1781 and was translated for distribution outside of France. It was, Soll remarks, one of the most successful works of all time.

Why? Because it rendered things public.[v] If the Nimblex permitted a visible accounting system that was nonetheless private, only to be brought out in cases of dispute, the Compte Rendu brought visibility to the masses. It thus brought the appearance of accountability—and a very public accountability. The suggestion is that nothing is kept secret, even if the system is only a shadow of the transparency and accountability it promotes. And more retrospective than prospective, it did not guide action so much as report on past action, showing a record of prior decisions. Its circulation throughout all of France—and indeed the world—contributed to a political restructuring in the form of a revolution.

3. Mist, the Ethereum client prototype



Mist is a prototype of the end-user client for Ethereum (the final client may look and work differently). Mist provides a place to browse the Ethereum community's collection of code: to join, invoke, and manage crypto-assets. The client enables the user to manage multiple identities and multiple sources of funds (just like MMM, the source of funds is visible but private). And like the publication of accounting manuals, the browser sets in place a standard to create a reliable, trusted set of ledgers (or code blocks running on a blockchain). The same suggestions of trust, honesty, and contractual rationality we saw in the standardized rows

and columns of MMM and the Compte Rendu are here manifested through multiple user interface features: the user cross-references the hash value[i] of a contract to confirm that the code has not been altered (unlike the 'blind' systems of shrink-wrapped software), a scalar 'trust value' is assigned, and a corresponding alert icon establish the highly visible symbols of trust.

Let's follow developer Alex Van de Sande's example of an Ethereum marriage contract. Van de Sande reimagines contractual fine print, since "everyone knows" he suggests, that the fine print "is to protect the… producer, not you." In its place, legal analysis of contractual fine print is transformed into a code audit (prompting some lawyers to speculate about a need for new legal skills), which readjusts the dynamic of power from the state or corporation to a liberal subject. Like MMM, the suggestion is that nothing is left secret—all is visible for evaluation and auditing. Fact-power control! The problem with this view, however, is that the code for the contract is as likely to hide secret clauses or tricks as it is to be meaningfully transparent. When Szabo originally introduced the concept of smart contracts he did not see "smart fine print" as a benefit of the system. It was rather a liability. To overcome opaque and complicated code Szabo suggests that "transaction semantics" in smart contracts need good visual metaphors to aid in their interpretation, adding to their transparency.

Mist is the simple front-end to the complicated Ethereum system, and is an important part in the developers' goal to democratize contracts. By providing powerful tools for peer-to-peer contracts the developers seek to displace transactional costs from fees and the cost and time associated with hiring legal professionals. Instead of requiring an official to verify signatures, Mist applies a cryptographic public key from a corresponding private key associated with a pseudonym. In doing so Mist is carrying on the tradition of "dematerializing" notaries and other legal professionals, a tradition that Jean-François Blanchette (2012) previously discussed in the context of the French government's move to establish a notarial public-key infrastructure back in the late 1990s. In this case the French government accepted the cryptographic key as a representation of the notarial power ultimately invested in the *human* notary, who was responsible for actually verifying the contract. The apparatus of the state, the legal professionals, and the rights and duties all still existed, but the paper and pen were no longer needed. Ethereum goes much further than Blanchette's example, as it replaces the cryptographic doppelganger with a fully dematerialized verification method that can be conducted directly by peers without the interference of legal apparatuses.

In the example of an Ethereum marriage contract, the contractual apparatus is replaced by the Mist browser. Once the parties have decided to get married they invoke the appropriate code block and work across a series of horizontal pages to construct the steps of the marriage contract. In working from page to page (instead of scrolling to the bottom of a long page, as is typical in most online fine print) the Mist browser forces structure on the contract parties. This is a linear method of interaction that is used to slow the user down so that she may think carefully about each step, but it sacrifices easy reference from one part to the next. The most important part of the marriage contract is the Serpent code that will run on the blockchain.[ii] The developers make a big deal about the Serpent code being "easy to read." In the screenshot above a portion of the sample code reads:

```
MaxWithDrawDaily = 0.01
MaxDurationOfInactivity = 365
MinAgeOfMaturity = 12
if msg.data[0] == 0:
id = msg.data[1] * 2 ^ 128
if contract.storage[id]:
return(0)
contract.storage[id] = msg.data[2]
contract.storage[id + 1] = msg.data[3]
contract.storage[id + 2] = block.timestamp + msg.data[4]
contract.storage[id + 3] = id + 5
return(msg.data[1])
```

Your typical traditional marriage contract, on the other hand, is authorized by state or religious officials permitting the participants to join in an "honorable state of matrimony" (or something along these lines), and it is date-stamped, and likely registered with a government entity. It is also not usually solely concerned with the disposition of collective property as this one seems to be—although that, of course, is deeply embedded in its history. The traditional performance of saying "I do" in marriage is, in the Ethereum contract, we suppose, the return() callback invoked in the Serpent code. The dynamics of contract execution in Mist are very different from the familiar ones embedded in existing social contexts. The challenge facing the construction of the Mist browser is to somehow replicate these complicated social forces while also enabling new functionality—functionality that currently exists in a software development paradigm and is foreign to social forces implicit in the history of contracts.

By signing a piece of paper in the eyes of witnesses and a legally-authorized officiant, and filing the paper with a government organization, the marriage contract becomes a record alongside others. The Ethereum blockchain takes on this role as record-keeper, but substitutes a decentralized database for a state archive. So long as the Ethereum community maintains the blockchain there is persistence and preservation, but on the flip-side this means Ethereum contracts are susceptible to invalidity through obsolescence and boredom. If the electronic network were shut off, or if everyone moved on to a new system, there is no paper-based backup archiving the existence (or execution) of these contracts. This isn't necessarily as scary as it sounds, though. Many researchers now realize that human sustenance is necessary for long-term preservation of *working* artefacts. Even the 10,000 Year Clock, shrouded in a mountainside, expects (although does not require) the occasional visitor to wind the bells. Software preservation necessarily requires continuous format updating, and greatly benefits from a healthy cadre of activist-preservers who may alter or even "remix" the software to keep up with the times or to form "living" derivations as Takhteyev & DuPont explain. Sticking a boxed copy of software in a display case is not a

solution to long-term preservation, and we need to realize that human use is probably our best chance for preserving complex systems of software.

The rub, however, is that high technology is famously faddish, so whether the network of miners will keep your Ethereum marriage contract as long as your love remains is an open question. Furthermore, because blockchain technologies are fundamentally cryptographic in nature, they have an additional preservation challenge. Cryptography is brittle: if even a single bit is changed (or "rots") the hash function no longer precisely refers to the contract, leaving only a nearly-impossible mathematical needle-in-the-haystack search as redress (formally, "code cracking"). These errors are mitigated somewhat by the distributed nature of the blockchain, but errors propagating across the network and simple coding mistakes (as we saw with Bitcoin in 2013) remain realistic concerns. Since redress is built in to Ethereum (or, really, doesn't exist at all since no breach of contract is even technologically possible here), broken code results in a formally invalid contract. In the eyes of the Ethereum blockchain, divorce may become programmatic and accidental.

Ledgers, Contracts, and Incentives

It does not take that much effort to see ledgers and contracts as part of the same modern assemblage. The latter has been dependent on the former, so perhaps we should not be surprised to see them popping up together in blockchain universes. Contracts between business parties rest on ledgers like title records, bank statements, lists of shareholders or ownership stakes, inventories, and the like, and depend on time-stamped verification of those records. The first difference between traditional ledgers and Ethereum is that Ethereum builds other things into the ledger. For the Nimblex and the Compte Rendu, those other things—contracts, revolutions—take place *outside* of the ledger. And those other things depend on other people to help create and execute them. The accountant is not doing all the work; there is also the lawyer and, possibly, the judge or arbitrator.

The second difference is that the persistence and verifiability of the Nimblex and the Compte Rendu were based on physical technologies and operations of recording. Now, we are not just drawing a distinction between the physical and the digital.[viii] We are drawing a distinction in terms of the effort involved in maintaining the ledgers. Presumably, if I use one of Moore's Modern Methods, or if I am the King of France, I pay my accountants to keep up the books. But if they quit or die, the materiality of the record endures, ready to be picked up by the next accountant, or filed away somewhere. Even if the people go away, the records still maintain their persistence and verifiability.

What about a blockchain? Earlier we referred to boredom. Without a community of computers running the protocol and engaging in transaction verification, the system stops working. Things can start to get out of control. Multiple chains of transactions can start to grow and the authenticity of the now-multiple records is thrown into doubt. The physical ledgers we have been discussing solve this problem with paid employees and paper. Bitcoin solves it with "mining," the incentivization of transaction verification by assigning parts of the ledger to miners who, competing with each other, win the proof-of-work lottery. Incentivization is critical to ensure that miners do not grow bored and stop mining, thereby

failing to provide the essential verification mechanism. Without a network of miners the blockchain itself may even cease to exist, and with no blockchain there is no ledger and its history of transactions. Much as with old-time physical world mining: you're all digging, digging, but sometimes, eureka!, you strike gold. That is what keeps you digging.

The introduction of contracts is potentially changing the blockchain ecosystem. By shifting from cryptocurrency to cryptocontract, it changes the incentive structure for ledger verification. Instead of getting money for verifying transactions, as with Bitcoin, you will now get "ether" (in Ethereum), the fuel of the system, which is also described as a "token," borrowing language from the Colored Coins Whitepaper. Tokens are the reward for doing the work of ledger verification. One does not strike gold with tokens, and therefore tokens provide fewer incentives for verifying transactions. We think we are seeing a discursive shift from mining to tokens. We also think that this is significant.

Szabo and Buterin both model the token basis of smart contracts in blockchains on game-theoretic "Schelling" or focal points. Focal points are a way of understanding how two parties can come to mutual agreement in an information-poor environment. Schelling offers the example of two people in New York who need to meet in an undetermined location without having prior communication or the ability to 'contract' a mutually agreed location. On game theory assumptions, each party will pick Grand Central Station (or, at least, will sometimes do so), because in a world in which many possibilities are equally likely, humans might look for patterns or unusual focal points of reference—the assumption being that if I think Grand Central Station is a good meeting spot the other party may think the same. Buterin offers the example of a fabricated incentive structure where two people will earn money if they are able to pick the same number from a list of numbers without communication or collaboration. People will, according to the theory, look for something—*anything*—that makes one number stand out—perhaps an even number, or a number with many zeros, or a well-known lucky number. Sometimes, so it goes, both parties will choose "10" and by the miracle of focal points the parties will have contracted to their mutual benefit without prior communication. In the less-fabricated case of meeting in New York, there are actually a great many focal points—Times Square, One World Trade Center, Brooklyn Bridge, New York Public Library, who knows where else!? Thus, the chance of our two parties meeting in this example is low. The situation is similar to contract negotiations between a workers' union and a corporation, where both sides are recalcitrant and there are a lot of issues and too few shared interests and ideas. On the other hand, Szabo suggests that some focal points are actually quite obvious, or "hard" in his parlance—the price tag on a retail good is not usually an invitation to start haggling. In some cultures the stated price is such an invitation, but in ours the stated price functions as a hard focal point that greatly speeds contractual negotiations. No pay, no play, as they say.

So, the development of cryptocontracts such as Ethereum has precipitated a number of significant changes. Cryptocontracts tend to build social and functional properties *within* the system, whereas traditional contracts require a cadre of individuals to perform these things outside the contract. Ethereum has also shifted the incentive structure of existing blockchain technologies from mining to tokens, and consequently has introduced concerns for

verification and longevity. Concerns about alternatives to the trustless system offered by Bitcoin have not been lost on the developers of these newer systems; Ripple has an answer, Ethereum has an answer, but only time will tell. The shift to tokens is not without its benefits. Speed and efficiency are immediate technical benefits. Ethereum's use of tokens takes advantage of a model of contracts that employ focal points. Focal points, the theory says, enable mutually-beneficial contracts in a relatively trustless but incentivized environment.

An interesting thing has happened along the way—or has it?

Seen one way, self-executing smart contracts seem to miss the whole point of contracts: that, like promises, they are made to be broken. That is to say, contracts only really get interesting in their initial formation and in their potential for breach. Ethereum seeks to put boundaries around uncertainty to the point of snuffing it out. Contracts, by contrast, are all about managing uncertainty. And other work gets done alongside that management. Emile Durkheim's classic discussion of the non-contractual basis of contract drew attention to all the social effort backgrounded by the modern belief in the purity of contract. Durkheim wrote that "facts which are beyond volition" (207) are always involved in contracts. Further, it is in the play of these relations themselves that social action makes itself felt. For everything in the contract is not contractual. The only engagements which deserve this name are those which have been desired by the individuals and which have no other origin except in this manifestation of free will. Inversely, every obligation which has not been mutually consented to has nothing contractual about it. But wherever a contract exists, it is submitted to regulation which is the work of society and not that of individuals, and which becomes ever more voluminous and more complicated (211).

Stewart Macaulay, writing in the early 1960s, explained how these ever more voluminous and complicated social regulations of contracts, these non-contractual elements, were not only helping businessmen manage uncertainty but also maintaining good business relationships. The production of an abstract contract as imagined by the legal scholars against whom he was writing—and perhaps to be instantiated in Ethereum—missed the point that the market of contract production as such, with its atomistic individuals meeting in a zone of free flowing information available to all, simply does not exist. The real bazaar is nothing like the hypothetical bazaar where everyone has access to all the same information and the price mechanism can operate as the textbooks say it should. People in the bazaar do not search for the best product at the best price by assuming an omniscient position and taking in all the available information—nor do they use their feet and walk to every stall for the same effect. Instead, they conduct "intensive" not "extensive" searches, and make their best choice. Clifford Geertz explained:

Search is primarily intensive because the sort of information one needs most cannot be acquired by asking a handful of index questions of a large number of people, but only by asking a large number of diagnostic questions of a handful of people (32).

From this perspective, smart contracts are not contracts at all because there is no possibility of uncertainty in their execution and thus no compliance; strictly speaking they are just

automaticity created by the verification game. Buterin even admits as much about Ethereum: "I now regret calling the objects in Ethereum 'contracts,' as you're meant to think of them as arbitrary programs and not smart contracts specifically".

Seen another way, however, the code itself demands a kind of non-contractual basis of contract. As we saw, one of the ways in which blockchain-based contract systems work is via tokens or points rather than money earned through mining. Schelling points are based on expectations of what everyone else expects everyone else to do. The verification game itself rests on a kind of background common sense that sounds a lot like 20th century legal realist Karl Llewellyn's community of merchants all acting "reasonably" (see Maurer and Richland 2012). So, in this sense, smart contracts are just like other contracts in that they ultimately rest on a vague but widely shared (dare we say distributed?) common sense. Which is itself a cultural system or, as Durkheim had it, the "regulation which is the work of society". Smart contracts afford us an opportunity to reflect on the forces required to ensure their active constitution—in part these are technical affordances, surely, but importantly the social and psychological systems that make up the core of what smart contracts are dictate what they are able to do.

If there are Schelling points in Ethereum contracts, written in complicated Serpent code, they are "hard" points. Hard focal points, you will recall, are like the price tag on a retail good that greatly reduces the negotiation required for exchange. In fact, the focal points in Ethereum are so hard as to eradicate the very idea of being modeled as a focal point at all. The Serpent code does not expedite contract negotiation, but rather replaces the difficult social and psychological work of contracting with self-executing code. Schelling points do not require prior arrangement to arrive at a mutually satisfactory conclusion, but they do require a certain amount of slippage or slop in the world (the chaos of New York in Schelling's original example). In the case of smart contracts all the messy business and legal apparatuses have been pushed out of the way: discourse has become binary, and the conditions of exchange have been rendered into objects. The sacrifice of exchange that Georg Simmel (2004) discusses with respect to money—the "interposition of man and his object of demand"—is offloaded to mediating code and is hardly felt, if at all (and is certainly not a focal experience). In this case, Lawrence Lessig's simple and pithy phrase was right: "code is law" in that code *replaces* law. If we must insist on a game-theory model to capture the Ethereum wedding contract discussed above it isn't Schelling points, it is the prisoner's dilemma.

Second, the verification method is based on people incentivized by the prospect of gaining tokens. This is the shift from mining to tokens we mentioned earlier. We are still not sure what to make of this, and time will tell with systems like Ethereum whether anyone will do the work of verification for tokens in themselves. Right now, Ethereum's ether will be convertible into Bitcoin and sold on exchanges, thus entering into the currency space. But must it? And if it does not, that is to say, if it is not warranted by an economic incentive (nota bene, like common sense, a cultural system), will anyone still "play?" And, indeed, there is an element of gamification here. It is also Applied Behavior Analysis—the use of rewards, often tokens, to shape behavior—here taken to a new level, to run a supposedly self-executing system.

Again, is this new? Surely, there were economic incentives in the maintenance of the tools of Moore's Modern Methods, or the creation and use of the Compte Rendu. But anyone who has served as a clerk knows the simple joy of adding up numbers and finding that the account balances, or the reward that comes from the successful deployment of office filing supplies. Where some might decry the bloodlessness of smart contracts embedded on a blockchain, the reduction to zero of degrees of freedom in self-executing law-like services, we wonder about these simple pleasures of non-economic rewards to create the satisfaction necessary to keep such a system going… indefinitely? Well, at least for as long as the people and machines running such systems want to imagine themselves useful by doing so. The whole thing starts to seem less like the science fiction world of distributed autonomous agents and self-enforcing agreements made by machines, and more like a game of Go. That might not be a bad thing. So long as it does not turn into Monopoly.

Acknowledgements:
We would like to thank Taylor C. Nelms for comments on earlier version of this paper. Maurer's research on blockchains and law is supported by the US National Science Foundation (SES 1455859). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Further Reading:

Blanchette, Jean-Francois (2012) Burdens of Proof Cryptographic Culture and Evidence Law in the Age of Electronic Documents. Cambridge, MA: MIT Press.

Boellstorff, Tom (2008) Coming of Age in Second Life: An Anthropologist Explores the Virtually Human. Princeton: Princeton University Press.

Durkheim, Emile (1933) Division of Labor in Society. Glencoe, IL: The Free Press.

Geertz, Clifford (1978) The Bazaar Economy: Information and Search in Peasant Marketing. American Economic Review 68(2): 28-32

Latour, Bruno and Peter Weibel, eds. (2005). Making Things Public: Atmospheres of Democracy. Cambridge, MA: MIT Press.

Macaulay, Stewart (1963) Non-Contractual Relations in Business: A Preliminary Study. American Sociological Review 28: 1-19.

Maurer, Bill (1997) Recharting the Caribbean: Land, Law and Citizenship in the British Virgin Islands. Ann Arbor, MI: University of Michigan Press.

Maurer, Bill and Justin B. Richland (2012) Lex Llewellyn and the Tribal Tax Status Act: 'Fallible Gropings' in Law and Society. UC Irvine School of Law Research Paper No. 2012-78.

Poovey, Mary (1998) A History of the Modern Fact. Chicago: University of Chicago Press.

Simmel, Georg (2004): The Philosophy of Money, trans. Tom Bottomore and David Frisby, London: Routledge.

Soll, Jacob (2014) The Reckoning: Financial Accountability and the Rise and Fall of Nations. New York: Basic Books.

Takhteyev, Yuri and Quinn DuPont (2013) Retrocomputing as preservation and remix. Library Hi Tech 31(2): 355-370.

---

[i] The Ripple network relies on a digital token, XRP, to settle payments. FinCEN determined that XRP was a "money" and that Ripple had failed to comply with Bank Secrecy Act provisions to counter money laundering. The case was unfolding at the time of our writing.
[ii] The authors participated in a convening on Bitcoin and blockchain technology held at UC Irvine during which Mic Bowman of Intel Labs outlined these core characteristics of the blockchain. The event was sponsored by the Institute for Money, Technology and Financial Inclusion, which Maurer directs.
[iii] See Maurer (1997).
[iv] We are reminded of the problem of recourse by payments expert Carol Coye Benson, who, at the aforementioned convening in Irvine, raised the issue with reference to the payment card industry.
[v] See Bruno Latour and Peter Weibel, eds. (2005).
[vi] Hash functions accept arbitrary data as input and output a fixed-size unique "fingerprint" of the input. The guarantee of uniqueness is critical here and is made possible by a form of cryptography derived from "public-key" cryptography first invented in the 1970s.
[vii] Serpent code is one of several types of acceptable programming languages used to create Ethereum contracts.
[viii] On the perils of so doing, see Boellstorff (2008).

Quinn DuPont is a PhD student at the University of Toronto. He studies the intersections of code, new media, philosophy, and history, with particular attention to the role of cryptography in contemporary life. He may be contacted at iqdupont.com and @quinndupont. **Bill Maurer** is Professor of Anthropology and Law, and Dean of Social Sciences, at the University of California, Irvine. He studies money and payment technology, and is the author or editor of 8 books, including, most recently, Data, Now Bigger and Better! (Chicago: Prickly Paradigm). He may be contacted at wmmaurer@uci.edu.