Legally Speaking: Smart Contracts, Archival Bonds, and Linked Data in the Blockchain

Darra L. Hofman
School of Library, Archival, and Information Science
The University of British Columbia
Vancouver, British Columbia, Canada

***Abstract*— As currently understood and used, "smart contracts" are merely a means to execute the terms of a full legal contract. This paper, however, proposes the creation of a semantic legal layer to support blockchain based legal contracts. Some of the primary challenges to such an implementation, including the need to develop robust, jurisdiction-specific legal ontologies, and develop means to preserve the evidentiary character of records leading up and proving contract formation, are considered. Particular attention is given to the particular challenges posed – and purposes behind – the use of legal language in contract drafting, with consideration of ways to utilize distributed ledger and linked data technology to leverage that specialist language for a broader base of contracting parties.**

Keywords—blockchain, smart contracts, archival bond, evidence, semantic layer, linked data

I. Introduction

"Smart contracts," in their purest form, seek to leverage the trustless, immutable nature of the blockchain to empower peer-to-peer, disintermediated agreements enforced automatically by code. Smart contracts, as such, are not legal contracts, but rather, code to allow systems to execute a legal contract. For example, in Solidity's "Introduction to Smart Contracts," it states that "a contract in the sense of Solidity is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain." The Solidity concept of "contract" includes necessary, but not sufficient, conditions for a full legal contract. However, the distinction between smart contracts and legal contracts is often obscured by the common name "contract," and the colloquial understanding of a contract as nothing more than a binding agreement. This paper explores whether, by integrating language, by way of a semantic legal layer, into blockchain-based smart contracts, smart contracts could become full legal contracts.

Despite the many jokes about "legalese," legal language is purpose-built, and functions as a code unto itself. The current blockchain landscape, in and of itself, is insufficient to capture the nuance of contract language, to preserve the evidence of the contracting process for those cases where parol evidence might be admissible, or to provide for the many non-financial terms that parties typically negotiate as part of a contract. However, the integration of a semantic legal layer – utilizing jurisdiction specific legal ontologies – could add the precision, flexibility, and enforceability to blockchain-based smart contracts to allow them to serve the same purposes at their traditional progenitors.

II. "Legalese" and its purposes

A. Law as Code

In the now-classic *Code*, Lawrence Lessig states:

> 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.[1]

However, if smart contracts are to fulfill their potential, it must be understood that, much as code is law, law is also code. While the Chamber of Digital Commerce views smart contracts as existing on a spectrum from pure (computer) code to a "natural language contract with encoded payment mechanism"[2], this view, however, understates the divergence of legal language ("legalese") from natural language.

As Alberts and Mollema note, legalese developed from "historical, sociological, political, and jurisprudential factors," and embodies not just terms, but legal thinking about those terms.[3] The end result is a specialist language which utilizes the same terms as natural language, but often with a very precise meaning that may or may not align with that of the natural language term. Furthermore, the "jurisprudential factors" mean that a legal term's meaning may vary from one jurisdiction to another. Take, as an example, "assault and battery." In natural language, the two terms are often treated as interchangeable. Legally, however, most jurisdictions distinguish the two. Assault, which can also be characterized as "attempted battery," consists of "any act of such a nature as to excite an apprehension of a battery may constitute an assault. It is an assault to shake a fist under another's nose." Battery, by contrast, "is commonly defined as a harmful, unlawful, or offensive touching."[4] Thus, assault is placing a person at apprehension of a battery. Unless, of course, one is in Kentucky, in which case, "assault" arises when one "intentionally or wantonly causes physical injury to another person."[5] While the differences are seemingly pedantic, the difference between an assault charge and a battery charge, with regards to penalties, can be literally years. The great specificity

978-1-5090-2991-4/17/$31.00 ©2017 IEEE

and power of legal language necessitates that, if smart contracts are to have the flexibility and import of their traditional progenitors, smart contracts must be able to draw on "legalese."

B. *"Contracts" Versus "Smart Contracts"*

The discussion of "smart contracts" on the blockchain has heretofore been dominated by technologists, often working from Nick Szabo's definition of a smart contract as "a computerized transaction protocol that executes the terms of a contract." While Szabo seems to have grasped the nuances of "contract" as a legal term, in subsequent usage, the "contract" in smart contract has lost much of its legal specificity, often used to mean some variant of "a binding agreement." While a contract is "a legally binding agreement," to rise to the level of "contract," an agreement must: 1. Arise as the result of *offer* and *acceptance* (discussed in detail in Section III, *infra*); 2. Include legally sufficient *consideration*; 3. Be between parties with the intent to contract; 4. Be between parties with the capacity to contract; 5. Comply with formal legal requirements (such as the Statute of Frauds) 6. Be legal (for example, one cannot contract to sell one's organs in the United States); and 7. Not be void (such as due to nondisclosure of material facts by one party).[6] One often sees these elements addressed perfunctorily in standard form contracts, including electronic clickwrap agreements. Courts have largely accepted such contracts as enforceable (although it should be noted that such factors as the relative sophistication of the parties or attempts to "bury" material terms have been considered in finding a particular contract unenforceable).[2]

Even in those cases where the above elements of a contract are satisfied, a smart contract without a rich legal vocabulary available to the contracting parties might well fail to meet expectations. In addition to the basic common law requirements for contract formation, a number of statutes also control the interpretation and enforcement of various terms. For example, commercial contracts in the United States are subject to the Uniform Commercial Code (U.C.C.). U.C.C. §2-201, the Statute of Frauds, requires that, "Except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker."[7] Whether or not a pure code contract would satisfy the Statute of Frauds is currently an open question; it would be upon the courts to decide if a smart contract is a "writing" "signed by the party against whom enforcement is sought."

Similarly, U.C.C. §2-314 imposes an implied warrant of merchantability for goods sold by a a seller who is a merchant of good of that kind, unless excluded or modified; this requirement, in short, places an obligation on sellers who regularly deal in a particular kind of good to ensure that their good is of "fair average quality" for that type of good in typical trade, unless the seller actively disclaims that warranty (for example, by selling the good "as-is"). Thus, even a seemingly simple contract encompasses far more than the direct transaction contemplated.

C. *But For A Comma, A Kingdom Was Lost*[1]

Integrating legal language into smart contracting processes, then, is no small feat. Particularly for contracts between major enterprises, smart contracts are highly unlikely to eliminate the need for legal counsel with expertise in both the industry(ies) and jurisdiction(s) pertinent to the contract. A number of clauses, such as choice of law, indemnification, disclaimer of warranty, limit of liability, assignability, termination, modification, and so forth, will still need to be negotiated between parties. For contracting parties without counsel at their disposal, however, fully legal smart contracts could potentially "level the playing field," giving them at least some access, through an ontology, to the same language used so effectively by attorneys, in addition to access to automated enforcement.

III. The Archival Bond, Semantic Blockchain, and Smart Contracts

A. *Blockchain and Linked Data*

Although the specific configuration of a legal semantic layer to support blockchain layers in novel, a semantic blockchain is not a new or unsupported proposal.[8][9] Ugarte offers three potential definitions of "Semantic Blockchain," of which we will consider the second: "Semantic Blockchain is a distributed database that maintains a continuously-growing list of standardized data records, using Resource Description Framework (RDF), hardened against tampering and revision."[9] Replace RDF with classification codes, and Ugarte's Semantic Blockchain is not far removed from the paper registries in which countless legal records – including, in civil law countries, contracts – are recorded.

Lemieux and Sporny make the case for the semantic blockchain explicitly on the basis of archival principles.[8] As they state, "the identities of the documents as records (i.e., evidence of facts about acts or transactions) are completely different by virtue of the different procedures of which they form a part (as represented by the archival bond). In the case of digital records, it would be impossible to prove that a record was an authentic representation (i.e., a copy) of another record, unless both items (the one to be proven authentic and the one that was reproduced) have unique identities. […] the archival bond must be made explicit and interpretable in order to ascertain the unique identity of each document as a record of the procedurally bound facts contained within it." [8]

This central archival purpose – explicitly preserving the identity of documents as records – is central to the records' later ability to serve as evidence of transactions. Rule 901 of the United States Federal Rules of Evidence requires "the proponent [of a piece of evidence] must produce evidence sufficient to support a finding that the item is what the

[1] Contract interpretation can turn on the seemingly picayune; a comma can cost millions of dollars. See, e.g., O'CONNOR v. OAKHURST DAIRY, No. 16-1901 (1st Cir. Mar. 13, 2017).

proponent claims it is," a requirement closely aligned to the archival definition of authenticity which, as ISO 15489, states that "[a]n authentic record is one that can be proven: a) to be what it purports to be, b) to have been created or sent by the person purported to have created or sent it, and c) to have been created or sent at the time purported."[10] Should one of the parties to a smart contract have issues with it after its formation or execution (for example, individuals who lost money in the DAO hack), that party would first have to prove the existence of a contract at all – a formidable feat for current smart contracts, which can easily be made without a legal contract coming into existence.

While using linked data to help preserve the archival bond in smart contracts offers a first step towards more enforceable smart contracts, full blockchain-based legal contracts are unlikely to happen without the integration of a legal ontology.

B. The Central Role of the Ontology

Lemieux and Sporny provide an explication of the role of the ontology in a linked data model for a blockchain system which is worthy of reproduction in its whole:

> The purpose of the ontology is to establish the context, including functional and procedural, of the transaction, which is a necessary precondition to render the archival bond among related records linked together by their participation in the same action. This ontology would ideally be created by domain experts in the area following specific procedures. The ledger data model and syntax make no assumption about which ontology is used. Ontologies can also be layered to enrich the expression of context. It is also possible to switch ontologies from block to block and object to object and to have an array of objects in which ontologies are switched for each object. It is by means of this mechanism that the archival bond can be established, since the entry can be linked by the ontology to the procedural action of which it forms a part in order to establish the record's identity (in this example – a real estate transaction) as well as being grouped into semantically meaningful classes for purposes of interpretation and retrieval.[8]

The development of appropriate ontologies to support full legal contracts on a semantic blockchain remains an open challenge. While there exist a number of legal ontologies, such LKIF-Core (an OWL ontology of "basic" legal concepts), a great deal more granularity would be required to properly support the use of smart contracts for full contracting purposes. Furthermore, legal knowledge, despite the vast array of code, cases, and statutes brought to bear, remains a largely tacit affair. To return to the example of the Uniform Commercial Code, even though Bagby and Mullen find codes such as the U.C.C. a good starting place for artificial intelligence and ontology work, they nonetheless find that simply examining the code itself "[misses] the rich experience of practitioner expertise that identifies key relationships and decision criteria."[11]

C. The Archival Bond and Contract Formation

As noted *supra*, a "contract" requires, at a minimum, *offer, acceptance,* and consideration. Offer and acceptance provide a particularly compelling test case for Lemieux and Sporny's design to preserve the archival bond in blockchain systems.[8] A contract does not exist until an offeree accepts an offer (while acceptance can be implied, it must always be active). Four principles[2] govern the validity of acceptance:

> "(1) It must take place while the offer is still in force, i.e. , before it has lapsed […] or been revoked.
> (2) It must be on the same terms as the offer. An acceptance made subject to any variation is treated as a counteroffer.
> (3) It must be unconditional, thus an acceptance subject to contract is not a valid acceptance.
> (4) It must be communicated to the offeror […] Telex, and therefore probably email, is equated with the telephone, so that communication takes place only on receipt."[6]

As Lemieux and Sporny assert, it is only by preserving the archival bond that the unique identity of each record can be preserved.[8] "The archival bond contains within itself the direction of the cause-effect relationship of the procedure which gives rise to records, and it is therefore the primary expression of the development of the activity in which the document participates, rather than just facts about the act that the document embodies."[8] Without the archival bond, it is impossible to know if a contract has formed, because it is impossible to reconstruct the relations of the records in such a way as to prove that an "acceptance" was actually an acceptance, as opposed to an attempt to accept a lapsed or revoked offer.

The archival bond is also critical in cases where the final reduction to writing of the contract between the parties is only a partial integration of their understanding. In such a case, "parol evidence," or evidence beyond the four corners of the contract, is admissible to prove the parties' intentions regarding terms beyond those captured in the contract. For example, if the final contract doesn't specify a time for performance, parties can introduce evidence of their negotiations regarding that term prior to the contract formation. Without the archival bond, however, it becomes impossible for the parties to clear the hurdles to admissibility for documentary evidence, namely, the best evidence and authenticity rules. Smart contract systems that don't provide for the archival bond leave any open terms largely to the discretion of the courts.

---

[2] These principles are general common law principles; statutory provision or contrary case law in a particular jurisdiction would have force in that jurisdiction.

IV. Conclusion

As the Smart Contract Alliance notes:

> It is not anticipated that smart contracts will displace the long-standing pillars of contract law (including offer, acceptance and consideration) in either situation. However, for smart contracts written entirely in code, courts will face additional challenges in applying contract law to determine when or whether a contract has formed, whether a party has performed its obligations, whether a party has breached and other related issues.[2]

Supporting smart contracts with a semantic legal layer, however, could help resolve many of those issues. For example, the Smart Contract Alliance notes the central role of notice in determine the courts' willingness to enforce terms in electronic contracts; they note the particular challenge that parties might face in proving that notice was given in a pure code contract. If such a contract were supported by a semantic legal layer, however, in which parties reduce to writing not just the transaction, but such terms as choice of laws, limitation of liability, and disclaimer of warranty, supported by robust linked data that preserved the archival bond of the records leading to contract formation, it's possible to imagine not just "smart contracts," but blockchain based legal contracts. While substantial research and work remains to be done before such a system could be realized, the potential gains in efficiency, clarity, and the return of power to individuals (as compared to "shrinkwrap," "boilerplate," and "clickwrap" contracts) are huge.

Acknowledgment

Much gratitude to Steven E. Richardson for helping me develop and refine many of the ideas behind this paper (although, of course, any terrible ideas are mine and mine alone), and for the "assault/battery" example. Aether and glitter, my friend.

References

[1] L. Lessig, "CODE version 2.0," *CODE version 2.0*, pp. 1–424, 2006.

[2] S. C. Alliance, "Smart Contracts : 12 Use Cases for Business & Beyond," 2016.

[3] M. Alberts and N. Mollema, "Developing legal terminology in African languages as aid to the court interpreter: A South African perspective," *Lexikos*, vol. 23, no. October 2011, pp. 29–58, 2013.

[4] A.2d, *Claggett v. State*, vol. 670. 1995, p. 1002.

[5] *Kentucky Revised Statutes 508.030*. 1982.

[6] O. P. Reference, *A Dictionary of Law*, vol. 20, no. 4. 2003.

[7] A. L. I. Uniform Law Commission, *Uniform Commercial Code*. .

[8] V. L. Lemieux and R. S. West, "Preserving the Archival Bond in Distributed Ledgers : A Data Model and Syntax," 2017.

[9] H. E. Ugarte, "A more pragmatic Web 3.0: Linked Blockchain Data," Bonn, Germany.

[10] International Organization for Standardization, "ISO 15489-1:2001, Information and Documentation - Records Management - Part 1: General," *International standard*, 2001. [Online]. Available: http://www.iso.org/obp/ui/#iso:std:iso:15489:-1:ed-1:v1:en.

[11] J. Bagby and T. Mullen, "Legal ontology of sales law application to ecommerce," *Artif. Intell. Law*, vol. 15, no. 2, pp. 155–170, 2007.