Enforcing Legal Smart Contracts

Published on August 22, 2016

Nina Kilbride | Follow
Head of Legal Engineering, Eris Industries

Blockchains smart contracts are a breakthrough development in the quest for a secure, interoperable technology to create data-driven solutions and conduct global commerce. This article outlines a beginning, multi-step framework for smart contract enforceability.

- **Blockchains for legally significant relationships.**

Blockchain software architecture combines the security of cryptography with the resilience of distributed networks to create chain of authentic, reliable information about data-driven relationships. This process creates a permanent ledger of transactions that may be viewed by all participants in that particular blockchain system. Blockchains may be configured to suit multiple purposes across multiple verticals, enabling collaborative data solutions. The digital future includes a multitude of blockchain solutions with interoperable *smart contracts* providing the rules by which data-driven relationships operate.

Blockchains deliver proof of who did what when, what lawyers call *evidence*. They add to the legal engineer’s toolbox the groundbreaking element of data certainty, the ability to rely upon the authenticity and chain of title of a document stored in decentralized, cryptographic architecture. This seemingly small feat, proving documentary conditions, consumes a large amount of lawyer time in the form of authentication of records, establishing findings of fact and auditing past events.

Smart contracts are automated, logical, cryptographically secure processes acting on blockchain data. By combining certain evidence and rock-solid audit trail, smart contracts can automate legally significant actions based on if-then/if-else logic, saving significant time and money. They will enable automation of many everyday, business-as-usual commercial processes.

Despite enormous potential benefits, stakeholders are unlikely to transfer their valuable business from legacy infrastructure to blockchain systems without firm assurance they are not sacrificing any hard-won existing legal rights in exchange for smart contract efficiency. Legal engineers building blockchain systems must carefully consider the pre-existing judicial precedent and regulatory structures that govern potential use cases.

Judicial enforcement of electronic contracts

A common refrain in blockchain industry reporting is a lack of legal standards providing guidance for those who want to deploy a smart contract-based system. From a former law practitioner's perspective, this perception is generally incorrect. For many use cases, ample authority exists to conceive and build smart contracts within existing legal principles.

For smart contracts, the existing body of electronic signature and records law provides both enabling and regulatory frameworks that give legal engineers a baseline starting point. Legally significant smart contracts must meet or exceed existing standards for electronic contracts.

Electronic contracts have been vital parts of international commerce and finance since the end of the twentieth century, when many governments enabled electronic contracting through the authorization of electronic signatures. The e-signature language of the United States' Electronic Signatures In Global and National Commerce Act ("E-SIGN") contains typical language:

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

In other words, if the terms of an electronic contract are otherwise binding, an electronically signed contract meets signature requirements, therefore legal obligations may exist in dematerialized, electronic form. Similar rules were adopted by forty-eight U.S. States as part of the model law Uniform Electronic Transactions Act ("UETA"). Across the globe, jurisdictions wishing to participate in the potential of electronic commerce over the internet enacted laws authorizing e-signatures.

A signature is often a requirement for enforcement of legal contracts, so recognition of e-signatures created the opportunity to transition many kinds of enforceable legal relationships to electronic format. Enforceable e-signatures enabled the creation of many kinds of electronic agreements and the ability to trade them worldwide, including consumer contracts, service agreements and financial instruments.

While e-signature law is largely uniform,there remains a significant degree of variation at the local jurisdictional level as to what agreements still require a traditional, pen-and-paper signature. For example, wills are excluded from most e-signature statutes. Real property records often require signed paper. Local variations are significant but not insurmountable hurdles to automated electronic contracts, underscoring the need for careful examination of specific laws when developing smart contract systems.

Electronic contracts are increasingly important elements in commerce today. Courts regularly enforce electronic agreements. Dematerialization and interoperability of contracts and instruments is encouraged and mandated by regulatory authorities. The e-signature laws of the turn of the century are updating with more sophisticated tools. The foundation for enforceable blockchain smart contracts is strong and well-placed, ready to support innovative legal models.

Blockchain smart contracts are fit for purpose as transferable records

The legal engineering inquiry into smart contracts systems does not end at judicial enforceability. Smart contract applications must comply with existing requirements for analogous electronic documents. Specifications and standards for systems that maintain data-driven relationships are produced by multiple actors like governments, regulators and ratings agencies. Read together, they are the framework that allow the transformation of e-contractual obligations into electronic securities and derivatives. Blockchain smart contract systems can be configured to meet and exceed existing requirements for encryption, data integrity, audit trail and security, trimming operational costs while enabling new revenue models.

One foreseeable blockchain application is creation and management of enforceable smart contracts. Enforceable contracts become assets that may be *securitized*, i.e.

treated as collateral, and/or traded. This process is a core function of existing electronic contract systems.

In the United States, E-SIGN and UETA provide similar standards for creation and storage of transferable electronic documents, while other regulations like the Uniform Commercial Code ("UCC") and securities law provide further guidance for specific collateral types. One initial issue is whether blockchains can meet these statutes' general requirements that a "single, authoritative copy of the transferable record exists which is unique, identifiable … and authentic." While it may at first seem counter-intuitive that a system based on a database existing at multiple nodes on a network creates a "single, authoritative copy" of a legal record, blockchain technology both satisfies and exceeds existing standards.

Blockchain smart contracts meet this standard via *cryptographically secure content-addressable storage*. In a process called hashing, data is passed through complex equations to produce a unique identifier. The hashing process is one-way, meaning no two sets of data produce the same outcome, and it is infeasible to decipher the hash to reveal the contents without a key. The distributed ledger provides the requisite immutability and audit trail.This combination produces the unique record of provenance, authority and control required by existing law, exceeding the capabilities of prior technology.

Blockchain technology fills the express needs for better electronic contract solutions. Both E-SIGN and UETA avoid making specific technological recommendations in order to encourage further innovation. UETA notes in comments to the 1999 model law that the statute

> *[I]s designed to allow for the development of systems which will provide "control" as defined in Section 16. Such control is necessary as a substitute for the idea of possession which undergirds negotiable instrument law. The technology has yet to be developed which will allow for the possession of a unique electronic token embodying the rights associated with a negotiable promissory note. Section 16's concept of control is intended as a substitute for possession.*

Jurisdictions are encouraging the use of blockchain technology to meet commercial data needs. As of this writing, the Vermont house is considering a bill that, among other things, treats blockchain documents as self-authenticating. Delaware has launched an initiative to use blockchains in many registry functions. U.S. federal authorities are considering explicit enabling of blockchain through legislation. Globally, this phenomenon is reflected in the many nations exploring blockchain solutions for government and commercial purpose. Blockchain smart contracts are are well-suited to bridge the gaps in worldwide data driven relationships

The existing body of electronic contracts law gives a firm foundation to the first step in creating automated legal contracts: *dual integration*.

The goal in drafting legal smart contracts is predictability of rules-based results that allow businesses to create reliable future plans and products. Traditionally, contracts may be made in any medium, including oral agreement. Enforcing oral agreements requires testimony of humans, an expensive and unpredictable process. Written contracts eliminate much of the uncertainty about enforcing a contract, because the terms are created at the time the contract is signed, not recreated from witness memory. The higher degree of reliability of paper writing led lawyers to develop a way to ensure that a contract means what it says and that it will be enforced as written: the *integrated agreement*.

An integrated written agreement embodies the entirety of the parties' contract. If a contract is fully integrated, evidence that would contradict or vary the terms of the written document is inadmissible, and a court is limited to the contract document in determining the intent of the parties.

Drafted properly, fully-integrated contracts may be proved solely by documentary evidence -- no testimony of humans other than document authentication is required or allowed. Well-drafted contracts contemplate potential disputes and provide evidence for managing those disputes as simply as possible. Cumulative lessons of potential outcomes become *boilerplate*, the fine print that addresses as many "what-ifs" as possible. A tightly-drafted, fully-integrated contract has no loopholes in its performance and prevents time and money wasted on enforcement. It has a high degree of predictability in its outcome.

To ensure enforceability of legal relationships made in in blockchain data relationships, the simplest first step is to combine an integrated, enforceable contract with smart contract functions via *dual integration*. Dual integration links smart contracts and full legal contracts by reference to the contract's storage address on the blockchain. Incorporating documents and objects by reference in legal documents is a familiar process to lawyers and delivers baseline enforceability industrial applications will demand.

Smart contracts can deliver today the reliability of existing e-contract procedures. Meeting existing standards enables us to iterate more complex smart contracts over time, creating safer, transparent assets, creating efficiency and liberating dark data. While Eris Industries is building increasingly automated legal contracts, since the company's inception we have recommended dual integration as a reliable, scalable way to build enforceable smart contracts

Self-enforcing smart contracts: the future of legal engineering

Due diligence of dual integration accomplished, legal engineers are free to explore the next frontier of smart contracts: self-enforcing contracts. Enforceability means the right to apply to an actor with authority over the contracting parties to force the breaching party to pay or act. One limitation of self-enforcing smart contracts is scope: smart contracts can only enforce agreements to the extent that assets are known and held within the blockchain system itself. Currently, a legal smart contract must be coupled with judicial legal enforceability in order to be useful. Absent legal enforceability, if a contracting party breaches an agreement, she may simply avoid liability by not placing value into the system against which a promise may be enforced.

However, it is foreseeable that there will be many situations where on-chain enforcement is a viable and desirable tool, for example, in cases where collateral is held in blockchain form, where disputes are primarily documentary, and for purposes of broader cross-collateralization.

Self-enforcing smart contracts, because of the variability in contracting procedures at local levels, are not yet amenable to a one-size fits all framework. Lawyers have long deconstructed deals and severed them into multiple, modular documents based on function. In order to create self-enforcing contracts, it is necessary for law-trained minds to deconstruct legal systems, actors, identities, property, governments, money and relationships. After deconstruction, legal engineers examine points in legal processes that may be augmented and automated through the application of smart contracts. In a legal process this means looking for objects, functions and deterministic, if-then/if-else logic to identify processes that can benefit from cryptographic data certainty.

The size of the legal engineer's undertaking is tremendous, but it is proportional to the commercial value of automation of contract provisions, decisions, and actions. The ability to apply logical legal processes to evidence using smart contracts opens the door to more complex legal agreements limited only by ability to define fact patterns and affect assets.

Tagged in: legal technology, contract law, bitcoin Report this

Nina Kilbride
Head of Legal Engineering, Eris Industries
14 posts

Follow

4 comments

Recommended ˅

Leave your thoughts here…

Mark Morris ··· 11h
All-Star -- Founder, lejer9.com -- inventor of the "Cognitive Blockchain" (tm)

Nina this is a good overview and intro to the current accepted norms. I would caution one to examine their frame of thought and ensure it is not weighted towards the current practices, because accepted practices will evolve with the efficiencies and rewards offered by a disruptive legal earthquake ushering in the ability to forge legally binding agreements between parties without the current horde of middle legal brokers whose purpose is foggy but intuitively unnecessary expense and baggage for the majority of legal agreements. 500 years of law has established a well heeled de facto library of legal thought, precedence, prose, and artifacts codified in print that will be digitized and assimilated into a legal "Cognitive Blockchain"(tm) capable of facilitating the legal needs of the profession, consumer, and regulators. I know this because at lejer9 we are building the "Cognitive Blockchain"(tm) and the legal industry is one of our target industries to massively disrupt. At lejer9 we are beyond the "smart contract" by several generations by introducing "Cognitive Contracts"(tm). This service facilitates the entire lifecycle of a legal agreement--draft, negotiate, enact, enforce, amend, dispute, and retire. They live and die on the lejer9 "Cognitive Blockchain"(tm). We see no difference between paper and digital paper, both managed by cognitive intelligence.

Like Reply | 1

Nina Kilbride ··· 3h
Head of Legal Engineering, Eris Industries

Interesting, Mark. We definitely will be able to make innovative legal solutions, but in order to get the freedom to do that, we have to deliver the existing degree of predictability provided by the law first. Otherwise I can't see any of my former clients even considering innovation. The law itself is not the problem - it's a priceless tool for the solutions people like you and me want to build.

Unlike Reply | You

Saurabh Goyal, FRM, CQF ··· 3d
Head of Trading & Risk Systems at Olam Europe Limited

So the blockchain will have the smart contract on it which will refer to a legal contract somewhere else. Is it safe to assume that since the legal contract is not on the blockchain, it is subjected to unauthorized changes?

Like Reply | 2

Casey Kuhlman ··· 2d
CEO at Eris Industries

This is why we prefer to log the hash of a pdf for the prose contract (legal contract). That won't change without the authorization process built into the smart contracts which are tracking the deal.

Like Reply

Nina Kilbride ··· 3d

Head of Legal Engineering, Eris Industries

Thanks for asking! The dual-integrated legal contract is on chain too. To the extent it needs changing, amendments, like in other kinds of contracts, will need to be included in the chain as well, all incorporated by reference.

Like Reply

Rocky E. M. Fikki ··· 2d

Experienced Environmental & Information Technology Executive, Visionary Entrepreneur, Business…

Here you can find a first look at some basic alpha examples of these sorts of Smart Contracts: https://github.com/androlo/doc-auth-multi and https://github.com/androlo/doc-auth

Like Reply

There is 1 other comment Show more.

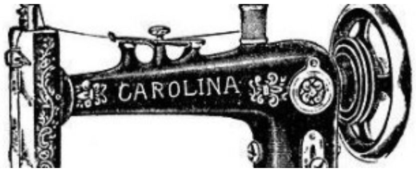
Don't miss more posts by Nina Kilbride

Ethereum's Killer App: Freedom of Contract

Nina Kilbride on LinkedIn

Blockchain's Secret Sauce: Legal Engineering

Nina Kilbride on LinkedIn



Patterns: Sewing, Machines, Law, Code and Learning

Nina Kilbride on LinkedIn

Looking for more of the latest headlines on LinkedIn?

Discover more stories

Help Center | About | Careers | Advertising | Talent Solutions | Sales Solutions | Small Business | Mobile | Language | **Upgrade Your Account**

LinkedIn Corporation © 2016 | User Agreement | Privacy Policy | Ad Choices | Community Guidelines | Cookie Policy | Copyright Policy | Send Feedback