

GUIDANCE NOTE REGARDING THE RELATION BETWEEN THE UNIFORM ELECTRONIC TRANSACTIONS ACT AND FEDERAL ESIGN ACT, BLOCKCHAIN TECHNOLOGY AND “SMART CONTRACTS”¹

Executive Summary

Recently, a variety of states enacted or considered legislation that amends the [Uniform Electronic Transactions Act](#) (UETA) to specifically address “blockchain” or “smart contracts.” Such amendments directly contravene the technology-neutral principles that have enabled the UETA to remain effective over the course of nearly two decades of technological change. In fact, rather than improve the UETA, these blockchain or smart contract amendments undermine the efficacy of the UETA going forward. In four parts, this Guidance Note explains that the UETA already adequately encompasses blockchain and smart contracts, and changes to specifically address these technologies are not only unnecessary but also detrimental. First, this Guidance Note provides an overview of the UETA and ESIGN, paying particular attention to the technology-neutral underpinning of both statutes. Second, this Guidance Note provides a high-level overview of blockchain-based smart contracts. Third, this Guidance Note dispels the myth that a smart contract is meant to serve, by default, as a legally enforceable contract. Finally, this Guidance Note analyzes blockchain and smart contracts under the UETA, demonstrating that the UETA, without amendment, adequately governs blockchain and smart contracts when incorporated into a legally enforceable contract.

UETA and ESIGN

In 1999 the Uniform Law Commission (ULC) approved the Uniform Electronic Transactions Act (UETA) to ensure that electronic signatures, electronic records, and contracts based or memorialized in electronic formats would not be rejected merely because of their electronic nature, for example, under a narrow reading of “writings” under state statutes of fraud. As the Prefatory Note to UETA states:

It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute—the substantive rules of contracts remain unaffected by UETA...

The Act’s treatment of records and signatures demonstrates best the minimalist

¹ The Uniform Law Commission Executive Committee approved the Guidance Note at its January 2019 midyear meeting.

approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law. These provisions are salutary directives to assure that records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.

UETA has since been enacted in 47 states, the U.S. Virgin Islands and the District of Columbia.

In 2000, the federal Electronic Signatures in Global and National Commerce Act (ESIGN; 15 U.S.C. 7001 et seq.) was enacted. Section 7001 tracks, in significant content, the basic provisions of UETA, while adding consumer consent provisions. UETA, however, contains additional provisions, not found in ESIGN, elaborating on how electronic signatures, records, and contracts are to be treated in the courts and elsewhere.

In a rather unique example of the interaction between state and federal law, ESIGN specifies that uniform enactments of UETA trump the provisions of ESIGN Sec. 7001. It further provides in Sec. 7003 that state enactments which are not enactments of UETA as finally approved by the Conference may avoid federal preemption provided they are consistent with ESIGN and do not require or provide greater legal effect to any specific technology or technical specification. Further, as to any such enactments after the effective date of ESIGN, the enactment must specifically mention ESIGN. For the purposes of this Guidance Note, the minor phrasing differences between the relevant provisions of UETA and ESIGN are irrelevant. This analysis of the relation between these commercial statutes and blockchain technology and “smart contracts” will proceed without regard to those minor phrasing differences because analysis under either or both UETA and ESIGN would lead to identical conclusions.

This Guidance Note is limited to the subject of the application of the UETA and ESIGN provisions dealing with electronic signatures and electronic records. It does not address virtual currencies, such as bitcoin or ether, which utilize blockchain technologies in their systems. Rather, the ULC’s 2017 [Uniform Regulation of Virtual-Currency Businesses Act](#) and 2018 [Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act](#) address some of the legal issues arising in the context of virtual currencies. Nor does this Guidance Note address potential issues in commercial law arising from various forms of electronic commercial paper, such as electronic notes. Those issues are being studied

by the ULC's Technology Committee and by the Permanent Editorial Board for the Uniform Commercial Code. Finally, this Guidance Note does not attempt to present a comprehensive explanation of blockchain technology, encryption technologies, hashing or time-stamping. It seeks only to provide sufficient information to enable interested parties to evaluate legislative proposals.

“Blockchain” and “Smart Contracts”

Legal, popular and business texts have been filled with articles about the potential uses of “blockchain” and “smart contracts.” Notwithstanding their prominence in current discourse, neither blockchain technology nor “smart” contracts is a new concept. A blockchain-based smart contract is computer code that is designed to write a state change to the underlying protocol upon the fulfillment of pre-determined conditions. The use of the term smart contract began with Nick Szabo in 1994. Szabo initially defined smart contracts as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”² For Szabo, the purposes guiding smart contract design “are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.”³

The computer code which is a smart contract may instruct a vending machine to deliver the product when payment is received, i.e., execute one or more operations that are a part of the bargain of the parties. In a more complex example, computer code may be transaction information in a blockchain to determine if and when all of the required conditions have been met before causing payment for an international shipment of goods to be transferred to the seller. Or the code may locate a vendor offering widgets, interact with the vendor's electronic agent [computer code] to negotiate the terms of a sale, and enter into an agreement for the purchase and sale of the widgets. Although in this last role the code may establish the “bargain of the parties in fact,” it typically operates in a pre-arranged system comparable to automatic bidding in automated security markets: there is automation, but only questionable autonomy.

² NICK SZABO, SMART CONTRACTS: BUILDING BLOCKS FOR DIGITAL MARKETS (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html; see also Nick Szabo, *Formalizing and Securing Relationships on the Public Networks*, FIRST MONDAY (Sept. 1997), <http://firstmonday.org/ojs/index.php/fm/article/view/548/469>.

³ *Id.*

Thus, although lawyers and other professionals frequently try to co-opt the term to always refer to some type of computer coded legal contract, the term smart contract, in fact, refers to a much broader set of software programs. In fact, Vitalik Buterin, the founder of the Ethereum protocol, upon which many smart contract-based applications are now deployed, recently lamented that “at this point I quite regret adopting the term ‘smart contracts.’ I should have called them something more boring and technical, perhaps something like ‘persistent scripts.’”⁴

Smart Contracts and the Legal Concept of Contract

The idea of a smart contract does not correlate with the legal concept of a contract. If a smart contract is any computer code that, when triggered, is capable of running automatically according to its pre-specified functions, rather than serve as the contract itself, the code may simply be causing the subject matter of a sales contract to be delivered or cause payment for another’s performance to be transferred. Those functions are related to contracts that may have been formed by the use of code, or automated agents, or by two human beings meeting face-to-face. A legal contract is something different. And because of those difference, Nick Szabo, the original inventor of the term ‘smart contract’ recently opined that “[w]orrying about whether a smart contract is ‘legally enforceable’ reflects a profound misunderstanding.”⁵

A contract is defined in the Restatement of Contracts 2d as “a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes a duty.” The common law of contracts requires two or more parties, each of whom is legally capable of being bound, a manifestation of mutual assent, and consideration. In the context of commercial law, the UCC defines a contract as “the total legal obligation that results from the parties’ agreement. . .” and an agreement as “the bargain of the parties in fact, as found in their language or inferred from other circumstances. . .”. Whether applying the common law of contracts as explained in the Restatement of Contracts 2d or the definitions of the UCC, the legal concept of contract is distinct from the concept of a smart contract. The legal concept of contract involves actions, or evidence of those actions, that result in an obligation to perform the duties that have been created. A smart contract, on the other

⁴ <https://twitter.com/VitalikButerin/status/1051160932699770882>

⁵ <https://twitter.com/NickSzabo4/status/1051606530108190720>.

hand, is computer code that may result in the creation of a legal contract, may evidence the creation of a legal contract, may constitute the performance of duties or execution of obligations, or may evidence the performance of duties or execution of obligations. In other words, as an initial matter, not all smart contracts or their use cases will fall under the definition of a contract at all, let alone within the scope of contracts and transactions to which UETA are applicable.

The Relation Between UETA and ESIGN, Blockchain and Smart Contracts

1. Electronic Signatures and Electronic Records

UETA and ESIGN establish a legal framework for all electronic technologies through broad definitions for electronic signatures and records and then basic provisions assuring that they are on a par with pen-and-ink for all legal purposes. These definitions commence in both UETA and ESIGN with the definition of “electronic” as “relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.” An “electronic signature” is “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” And a “record” is “information that is inscribed on a tangible medium or that is stored in a electronic or other medium and is retrievable in perceivable form.” An “electronic record” is a record that is “created, generated, sent, communicated, received, or stored by electronic means.”

UETA and ESIGN then proceed to provide, in relevant part, that:

- (a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- (b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- (c) If a law requires a record to be in writing, an electronic record satisfies the law.
- (d) If a law requires a signature, an electronic signature satisfies the law.

2. Electronic Agents

Whether used in the process of contract formation or performance, the use of computers to “act” for the parties is inherent in the concept of “smart” contracts. Both UETA and ESIGN expressly provide that a person *may* be bound by the operations of an electronic agent or in an automated transaction. UETA Section 14 explicitly states that a contract “may be formed by the interaction of electronic agents of the parties, even if no

individual was aware of or reviewed” the operations of the agent or the terms and agreements. It further provides that the same is true if the actions involved the interaction of a human and an electronic agent. E-SIGN Section 101(h) provides that a contract may be formed and is enforceable if it involves the “action of one or more electronic agents” so long as the agent is *legally* attributable to the person to be bound.

Federal Preemption and Technology Neutrality

Not only do UETA and E-SIGN definitions and provisions broadly provide that any electronic record, signature or contract may not be denied legal effect or enforceability solely because of their electronic nature, the UETA drafting committee considered carefully whether to call out specific technology such as PKI and enhanced authentication through digital signatures, including providing heightened deference or presumptions, but determined to maintain technology neutrality. E-SIGN further emphasizes the broad application, and technology neutrality, of both bodies of law by its provisions in Sections 102 and 103 outlawing any law requiring specific technologies or giving greater legal effect to specific technologies. E-SIGN Section 103 authorizes some state laws or regulations regarding specific technologies but imposes specific thresholds before such laws or regulations will avoid federal preemption.

The effect of this network of legislation is to provide a basic infrastructure for emerging technologies, one that assures that actions taken with an electronic base are not prejudiced regardless of the specific technologies employed. This framework has worked for the past two decades to support the continuing development and deployment of emerging technologies.

Issues Raised by Proposed Blockchain or Smart Contracts Legislation

1. Unnecessary or redundant legislation. Some proposed and enacted legislation has simply provided that blockchains or a smart contract be considered electronic signatures or records within the State’s UETA and thus not to be denied enforceability because their electronic nature. When considered in combination with the issue of inconsistent, and at times, technically narrow or incorrect, definitions discussed below, the complications posed by redundant legislation

become quite clear. In particular, there are many variants of blockchain technology, and it is likely that new ones will be developed over time. If one or more of those variants do not fall within the definition of “blockchain technology” enacted as an amendment to UETA, then arguably, smart contracts deployed on top of those protocols do not enjoy the protective presumptions of UETA. Given that the technology-neutral approach currently taken by UETA is broad enough to encompass blockchain technologies in its many variations, the result of enacting blockchain-specific amendments to UETA provisions is actually a significantly worse outcome for blockchain-based businesses.

2. Inconsistent definitions. Some of the proposed legislation contains definitions of either blockchain or smart contracts that are stated differently or are sometimes conflicting. Different attributes of blockchain technology have been advanced in public discourse. Definitions in legislation introduced in 2018 in California, Florida, Nebraska and Tennessee differ from those of industry groups and from each other. Rather than make these jurisdictions blockchain-friendly for start-ups and entrepreneurs, the variances in definitions actually introduce legal uncertainty where it did not previously exist, and invite unnecessary and expensive litigation.
3. Threat of federal preemption. This threat comes from two sources. The first is the existing, overriding provisions of E-SIGN which require that any state law dealing with electronic records and signatures be consistent with E-SIGN and not provide special effect to any specific technologies. The second is that inconsistent, conflicting state laws may provide incentives for Congress to preempt those state laws in order to ensure that states do not hinder or burden interstate commerce.

The preference of the ULC is to maintain the uniformity of UETA, which has been one of its most popular statutes and has been referenced in all subsequent ULC products in which electronic signatures and records may arise. We ask that state legislators balance the greater business and legal certainty of uniformity against any perceived need to recite two technologies that are yet to be consistently defined.