STEPTOE BLOCKCHAIN BLOG

Steptoe
STEPTOE & JOHNSON LLP

The Enforceability of Smart Contracts

By Alan Cohn, Travis West and Chelsea Parker on May 4, 2017
Posted in Smart Contracts

This is the first in a series of posts that breaks down our article, "Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids," recently published in the Georgetown Law Technology Review. First, we will discuss the enforceability of blockchain-based smart contracts followed by four use cases: simple insurance contracts, parametric insurance, smart meters, and microgrids. You can read the full article here.

Smart contracts have the potential to impact a range of industries, and some are even calling 2017 "The Year of Smart Contracts." Smart contracts can be used not only to automate existing processes, but also to create new industries and reach new markets. By providing a digital platform for coding "if-then" statements, providing a secure and resilient environment for value transactions, and preserving a detailed and immutable transaction history, the blockchain provides an ideal platform for smart contracts.

With companies and industries continuing to explore new blockchain-based smart contract applications, it is important to establish their enforceability.

Numerous questions have already been raised as to whether a contract on the blockchain is binding and enforceable. Vermont, for instance, has made multiple attempts to pass a law that would make blockchain evidence self-authenticating, and has finally succeeded in enacting one. Arizona recently passed a law clarifying that signatures obtained through blockchain technology are valid electronic signatures. We believe that the federal Electronic Signatures in Global and National Commerce Act ("ESIGN") and state laws modeled on the Uniform Electronic Transaction Act ("UETA") provide sufficient legal foundation for blockchain-based smart contracts to be enforced under current law.

Development of UETA and ESIGN

In the early days of the internet, states enacted a patchwork of laws designed to balance the needs of online commerce with protections of consumers and businesses. In response to the often-contradictory state laws, the National Conference of Commissioners on Uniform State Laws ("NCCUSL") drafted UETA to provide a model law to harmonize the rules governing electronic commerce transactions. Currently, forty-seven states, along with the District of Columbia and the U.S. Virgin Islands, have enacted some form of UETA.

Despite the UETA's purpose of providing a standard national code governing electronic commerce transactions, states inconsistently implemented UETA by changing several provisions to protect consumers or reflect their own state laws. Businesses, again facing the challenge of needing to comply with multiple inconsistent state laws, pushed for a new law to standardize the equivalence between electronic signatures and other forms of signatures on a national level.

Congress responded by passing ESIGN, which, while mirroring UETA in many ways, diverged in some others, including consumer consent requirements. However, Congress included a pre-emption provision that gives states the option to choose between ESIGN compliance or UETA adoption. Congress specified that states could preempt ESIGN with their own laws, so long as those laws were either UETA or did not conflict with ESIGN. This reflected the desire that states either follow ESIGN or adopt UETA. In this way, the preemption provision ensures that either ESIGN or UETA governs electronic transactions.

Common Provisions of UETA and ESIGN

UETA and ESIGN share several features. First, both guarantee that a signature or record will not be held legally ineffective because it is in electronic form. Second, both clarify that any law that requires a record to be in writing will be satisfied by an electronic record. Finally, an electronic signature is held to be the equivalent of a written signature for any law that requires a signature. Collectively, these provisions ensure that electronic records and signatures carry the same legal authority as physical documents and signatures.

These provisions also recognize the notion that consent can be granted by electronic means. UETA requires that both parties agree to "conduct transactions by electronic means," which can be "determined from the context and surrounding circumstances, including the parties' conduct." ESIGN and UETA also have sections relating to the retention and accessibility of any electronic records. Both acts require that an electronic record be producible and accurately reflect the final form that the parties agreed upon.

Overall, the effect of UETA and ESIGN is to allow digital signatures to have the same effect as a physical signature. Congress wanted to allow businesses to benefit from the efficiency of transmitting and signing documents electronically and to free businesses from being required to keep a warehouse full of contracts. Although it is difficult to imagine now, the Congressional Record is replete with the concern that electronic signatures would somehow be less valid than physical signatures unless Congress acted. The courts have interpreted both the UETA and ESIGN in a way to help facilitate digital transactions, which has allowed the digital economy to grow. Indeed, UETA and ESIGN have allowed credit card applications, loan applications, and other transactions to be performed online while still being enforceable.

How Do UETA and ESIGN Apply to Blockchain-Based Smart Contracts

The key to the applicability of UETA and ESIGN to blockchain-based smart contracts is the cryptographic key with which blockchain-based smart contracts are signed and acknowledged. From our perspective, asymmetric key encryption falls squarely within the both the language and intent of ESIGN and UETA as an "electronic signature."

In short, one way for a party to express agreement with the terms of a blockchain-based smart contract is to provide its digital signature utilizing a cryptographic key. This signature, expressed using the blockchain's asymmetric key encryption, is similar to the initial digital signatures that early forms of UETA envisioned. UETA defined "electronic signature" as "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." An electronic signature therefore has two components: the signature, in whatever form it is, and the intent to sign.

Courts have interpreted the requirement for the signature and the intent to sign broadly. For example, courts have found that typing "Thanks" plus the sender's name in an email constitutes a signature. The court in that case noted that the plaintiff manually typed her name, as opposed to having a default signature automatically attached by her email program. This is a low bar to set to allow UETA to enforce the contract.

By contrast, parties using blockchain-based smart contracts would negotiate terms and then each party would need to use their cryptographic key, unique to them, to sign off on the contract. The cryptographic key would be either a "symbol or process attached to or logically associated with a record," and the deliberate signing off would demonstrate each party's "intent to sign the record." Regardless of the specific contract terms, the fact that a blockchain-based smart contract can require the participants to sign the contract through the cryptographic key should assure courts that a blockchain-based smart contract is a legally-binding agreement under UETA and ESIGN.

Moreover, a blockchain-based smart contract can prevent some of those factual challenges because the cryptographic nature of the signature for a blockchain-based smart contract can more effectively establish a person's identity. In a case arising out of Louisiana, a court upheld the applicability of Louisiana's version of UETA to automobile insurance contracts but held that a genuine issue of fact existed over whether the plaintiff had actually signed the insurance waiver (Bonck v. White, 2012-1522 (La. App. 4th Cir. Apr. 24, 2013); 115 So. 3d 651, 655). The insurance company insisted that she had, but she pointed out that the waiver was signed four days after she met with the insurance agent to apply for insurance. Due to this conflict, the case needed to go back to the trial court for further proceedings. This is not an uncommon issue, as similar cases have arisen in other jurisdictions. These kinds of disputes often boil down to which side can muster enough evidence that the proper person signed the contract or create enough doubt to go to trial, where a jury could be swayed by other concerns.

A blockchain-based smart contract, by contrast, needs to be signed by each party using a cryptographic key that only each party has access to. This cryptographic key is a much more reliable identifier, as it is nearly impossible for someone to forge the key. A third party can see that signature and immediately know who signed it, preventing many disputes about the authenticity of a signature. A party may argue that its cryptographic key was stolen, but the key is unlikely to be stolen because the benefits of stealing the key for an insurance contract or other type of blockchain-based smart contracts are small. In the case of an insurance contract, the beneficiary could not be changed without needing a new smart contract, and the smart contract would ensure that the premium is being paid, which lessens the chance a party could enter into a fraudulent contract. Instead, the cryptographic signing would function much like having witnesses observe the signing of a will. It would create a high barrier to overcome and reduce costs of enforcement because fewer parties would be willing to go to court to contest that they signed a contract with such strong evidence.