The Georgetown Law Technology Review

Articles

Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids

Alan Cohn, Travis West, and Chelsea Parker

April 2017

Cite as: 1 GEO. L. TECH. REV. 273 (2017)
Perma: https://perma.cc/TY7W-Q8CX

(Download PDF)

Before 2016, blockchain technology was known, if at all, as the technical underpinnings of virtual currency. However, in the past year, blockchain technology has come into its own. It is now seen as a groundbreaking advance that can both reduce frictional costs in existing transactional systems and enable new, previously-unworkable models of social and commercial engagement.[1]

A "blockchain," as the name implies, is in its simplest terms a "chain" of previously-validated "blocks" of transactions that constitutes an immutable digital ledger and the distributed, resilient foundation for transfers of value. However, the newfound attention to blockchain has come with an increase in the attendant hype. Blockchain technology threatens to become the "next big thing" and all sorts of blockchain-based projects are being proposed. For instance, the Republic of Georgia has committed to using the Bitcoin network to validate property-related government transactions,[2] and a private company in San Francisco has developed new pharmaceutical packaging technology that uses blockchain to reveal whether a package has been opened.[3]

These and other projects have led many observers to ask whether a simple cloud-based database could accomplish the same task,[4] while others have asked whether there are actually realistic and beneficial uses for blockchain technology beyond simply underpinning a digital currency.[5]

While centrally-administered cloud-based databases can accomplish many tasks, the crucial benefit of blockchain is the ability of the technology to enable transactions to occur in an environment where the parties do not trust each other and do not want to rely upon an intermediary. Blockchains are ideal for applications where transactions are transparent and no single user controls the rules of transaction; by contrast, a centrally-administered cloud database places a single entity in control of the rules of the platform, while also creating a central store of data that can be hacked or corrupted.[6] For instance, in places where land records are poorly kept or changed because of corruption, a cloud-based database run by a central government would not provide the requisite trust that an immutable blockchain system would.[7] For tracking important and critical materials, such as pharmaceutical drugs or food, speed and trust can be improved by using a blockchain-based tracking system.[8]

If blockchain can enable high-value transactions in low-trust environments, a logical next step is to use blockchain to automate certain aspects of those transactions. Indeed, current blockchain scripting language enables the programming of "if-then" statements in order to automate transactions on a blockchain. By doing this, the value being digitally represented on the blockchain—often thought of as a "token," like a digital coin—can be transformed instead into an instantiation of an agreement between parties that a transaction of value automatically take place upon the occurrence of a previously agreed-upon event or events.

Some have humorously noted that a "smart contract" is neither smart nor a contract, because it simply executes previously-written code, which itself was constructed to represent an actual contractual agreement. [9] Nevertheless, the promise of automating existing and new processes while also eliminating the middle person, smart contracts may emerge as one of the blockchain's "killer apps." [10]

But can blockchain-based smart contracts be recognized under law as currently conceived, and in what instance would this represent both a viable and a valuable usage? This Article examines these questions in turn. Part I of this article provides a practitioner's background on blockchain technology and blockchain-based smart contracts. Part II sets out the argument advanced by digitization experts that existing laws, specifically 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. Part III of this Article describes potential uses within the insurance and energy industries where blockchain-based smart contracts could be implemented under the legal framework of ESIGN and state UETA-based laws.

Part I: What is a Blockchain and What is a Smart Contract?

As noted above, a "blockchain," can be understood as a "chain" of previously-validated "blocks" of transactions that constitutes an immutable digital ledger and the distributed, resilient foundation for transfers of value. Underpinning that simple description, however, is a sophisticated digital protocol that includes complex cryptographic algorithms, public and private encryption keys, and a transaction validation process that results in a high-integrity ledger of transactions. Similarly, a "smart contract" can be understood as a digital instantiation of an existing contract. However, this is not the only definition of a smart contract, and indeed, blockchain technology enables different types of smart contracts. This Part I explains these concepts in turn.

Blockchain Defined

"Blockchain" can mean—depending on who you ask—an append-only database, an underlying technological protocol, or a virtual currency system. For the purposes of this Article, we use the term "blockchain" or "blockchain technology" to refer to a distributed, decentralized ledger that, when combined with a digital transaction validation process, allows for peer-to-peer electronic transfer of an asset without the need for an intermediary, such as a bank. [11] Blockchains replace centralized recordkeeping by having every participant in a blockchain-based process maintain an append-only copy. [12] Every participant can write to and view the ledger, but no participant can change the rules of administration. [13] This distributed ledger is synchronized in real time by a community of individuals (through their computers, or banks of computers) validating transactions. [14] This synchronization of recordkeeping prevents users from posting invalid transactions to the blockchain, such as trying to spend a resource that user has already spent, since the invalid transaction (e.g. a double-spend of a single asset) would be detected by the rest of the community by comparison to their copies of the ledger. [15] The validation of individual transactions is performed using different types of digital mechanisms—for example, the Bitcoin blockchain uses a proof-of-work algorithm [16]—and solutions to the proofs are verified by the community. [17]

As the previous paragraph implies, blockchain technology relies on a variety of digital processes to maintain the integrity of the system, including sophisticated cryptographic algorithms. Cryptography is the science behind protecting and securing information, typically in an insecure environment. Within the blockchain ecosystem, cryptography can be used to protect the identity of participants, keep transactions private, and confirm the authenticity of the transactions. A transaction is signed with a cryptographic key by the participants, which ensures that each participant validated it and prevents a third-party from impersonating one of the participants. The transaction is then encrypted in such a way that the digital signatures of the participants and the contents are all signed, so that no one can change any part without causing others on the blockchain to reject the transaction. Multiple transactions are added onto a block, which references the previous block via its cryptographic signature. [18]

The keys that are used to sign transactions are normally implemented using asymmetric encryption. In asymmetric encryption, each user generates a pair of keys that are linked through complex algorithms: one is a private key that the user keeps secret; and the other is a public key that, as the name implies, is publically available. [19] If a second user wants to share information with the first user, the second user can sign a document with the first user's public key, which will encrypt it in such as a way as to ensure that only the first user's private key can decrypt it. Conversely, the first user can sign a document using their private key. That document will only be able to be decrypted by the corresponding public key, which establishes that the encrypted document was signed by the first user.

Being distributed and open, the blockchain enables high-trust transactions without the need for an intermediary or third party since many parties are verifying each transaction. The Bitcoin blockchain, for example, ensures that transactions are validated by incentivizing validators with a small financial reward that is unrelated to the underlying transaction. [20] For popular public blockchains such as the Bitcoin blockchain and Ethereum, transactions are public, and identity is based on the user's public authentication key. By distributing copies of the ledger, the system is resilient and resistant to corruption or attacks on single or groups of nodes. [21] These characteristics enable blockchain to incorporate both security and resilience by design.

Blockchains can also be private or "permissioned." Permissioned blockchains are administered by a single entity, although other technical attributes common to open or permissionless blockchains remain the same. As the name applies, permissioned blockchains can be configured to restrict access or permissions to only approved users. Permissioned blockchains give administrators the right to both control access and require a higher degree of authentication. [22] Private blockchains are instantiations of similar technology in a fully private space, such as a private server or cloud-based environment. [23]

Blockchain technology has made noteworthy progress in the past year, from large banks and governments experimenting with the new technology, to newly formed consortia facilitating industry-wide exploration. [24] Over forty percent of senior executives at U.S. organizations with over $500 million in annual revenue believe blockchain will disrupt their industry. [25] While the financial services industry was one of the first industries predicted to be disrupted by blockchain, a range of industries, from life sciences and healthcare, to technology and media, are showing significant interest. [26] For example, over forty-two percent of senior executives at U.S. organizations in the consumer products and manufacturing industry with over $500 million in annual revenue are planning to invest $5 million or more in the next calendar year. [27] These investments are not just speculative, with twenty-one percent of the executives stating that they have already brought blockchain-based applications into production. [28]

Despite the technical differences between open, private, and permissioned blockchains, for the purposes of this Article, we will use the term "blockchain" or "blockchain technology" to refer to the technology generally, as each of these types of blockchains presents similar opportunities and challenges from a smart contracts perspective.

Blockchain-Based Smart Contracts

Smart contracts as a concept are not intrinsically linked to blockchain. "Smart contract" is often used interchangeably with a broad range of terms, from "smart legal contract" to "digital contract" to "smart contract code." [29] Generally, the definitions include some type of automated, self-executing transaction. [30]

A smart contract has multiple benefits over traditional contracts. [31] The digital nature of the contract ensures that there is a final version of the contract written in a detailed method that will be executed precisely by computers when necessary. Unlike a paper contract, which can be destroyed or exist in multiple versions, a smart contract will by necessity be saved and executed only according to its encoded instructions. By forcing the contract to be translated into computer code, a smart contract lessens the parol evidence problem, in part because a computer cannot consider any external evidence and can only run the code that it is given. It will be difficult for a party to argue that there were agreed upon but un-incorporated issues if that party signed and verified that the contract had been accurately translated into computer code. Even if the parties dispute the terms later, the smart contract itself becomes a powerful form of evidence that demonstrates what the parties thought they were agreeing to. [32]

Smart contracts are most efficient for contracts that can be reduced to simple "if-then" statements, as their terms are easy to convert to computer code and can be executed automatically. For instance, a life insurance contract can be coded as an "if-then" statement by specifying that if the policyholder dies, then payment to the beneficiaries commences. For similar contracts, given the option of a smart contract, it may no longer be efficient to have a person in charge of administrating and executing these contracts.

For the purpose of this Article, a blockchain-based smart contract is a contract between two or more parties that is stored and digitally executed on the blockchain using code. [33] While human involvement is needed to define the contract and input the code, the actual execution of the contract is automated based on a defined parameter, such as an event or price. [34]

Blockchain-based smart contracts have the potential to impact a range of industries [35] and some are even calling 2017 "The Year of Smart Contracts" for blockchain. [36] Blockchain-based 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. Blockchain technology allows users to write an agreement into code in the exacting detail required by both a court and a computer to faithfully execute only terms agreed to by the contracting parties. [37]

For the purposes of blockchain-based smart contracts, every action on a blockchain can be configured to require the participants to sign off on the transaction using their private cryptographic key. [38] This helps to create the record of transaction and verifies the identities of the parties involved in case of later disputes. Once a consensus is reached that a transaction is valid, the transaction is added as a block of multiple other transactions to the chain of previous blocks of transactions (hence, "blockchain"). [39] These blocks are then part of the ledger and cannot be removed or changed, giving the chain both transparency and immutability. [40] For instance, if a party later wants to edit or cancel a transaction, rather than removing that block from the blockchain, a new transaction will be formed and the underlying asset will be returned in that transaction.

Another essential element of blockchain-based smart contracts is the ability of the blockchain protocol, as a digital system, to monitor for events that would trigger the embedded "if-then" statement. Having every node□ each of which verifies the correctness of the blockchain simultaneously□ monitor external sources for the defined parameter is complicated, and entails certain risks. While there are a few possible solutions, oracles are a common solution. Oracles are one or more external digital agents or sources trusted by the blockchain participants. [41] The oracle monitors the external parameters designed within the smart contract, and gives direction or approval to execute the contract if those parameters are met. [42] An oracle can be configured to work with numerous blockchains, external sources, and any necessary entity involved with automating the execution of the smart contract. [43] Using an oracle or other triggering mechanisms, smart contracts will only execute upon the occurrence of agreed-upon events, based on agreed-upon sources of information. In this way, smart contracts have the potential to simplify administration of a range of commercial contracts.

Although blockchain technology is being explored in many areas, its usage in smart contracts has been among the most prominent. [44] The Ethereum blockchain was among the most popular blockchain implementations of smart contracts, due to its scripting language that could be used to write the contracts. [45] The native ability to generate smart contracts has led to a proliferation of startups using Ethereum, ranging from gambling contracts [46] to energy contracts. [47] Ethereum also has its own native currency, Ether.[48] Companies are also emerging to build enterprise-grade applications on the Bitcoin blockchain. Similarly, as with other open-source environments, third party companies are developing a range of applications for the Bitcoin and Ethereum blockchains and others, including applications focused on identity,[49] device authentication,[50] and transaction analysis.[51]

Recognizing the potential benefits of blockchain-based smart contracts, industry leaders have already started experimenting with new applications. $116 million was invested in smart contract venture capital-related deals in the first quarter of 2016 alone.[52] Governments and regulatory agencies are also experimenting with blockchain-based smart contracts. The state of Delaware created the Delaware Blockchain Initiative and is exploring the use of blockchain-based smart contracts to increase recordkeeping efficiency and reduce costs.[53]

Part II: Smart Contracts, UETA, and ESIGN

With companies and industries continuing to explore new blockchain-based smart contract applications, it is important to establish the enforceability of blockchain-based smart contracts. Technical details aside, questions have been raised as to whether a contract on the blockchain is binding and enforceable.[54] 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.[55] Arizona recently passed a law clarifying that signatures obtained through blockchain technology are valid electronic signatures.[56] It is not clear that Arizona was responding to any perceived problem with the enforceability of signatures obtained through blockchain technology; instead, the bill appeared to be a way for the state to signal that it is open to blockchain companies.[57]

Even if these contracts can be efficiently translated into computer code onto the blockchain, they will not help anyone if they are not legally enforceable. Contract law is a complicated area of law, with principles dating back to medieval England.[58] Disputes often arise about the interpretation of terms. For parties who agree upon a contract and then convert it to computer code, a dispute about a term in the original contract may now be compounded by a disagreement about its manner of implementation in computer code.

In this Part II, we argue that current laws, such as UETA and ESIGN, already allow for smart contracts to be enforced. Part II describes the evolution and application of state laws modeled on UETA[59] as well as the federal ESIGN.[60] Part II also describes how blockchain-based smart contracts fit under these authorities. Based on this examination, we conclude that blockchain-based smart contracts are enforceable under UETA and ESIGN.

UETA and ESIGN

A. 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.[61] Currently, forty-seven states, the District of Columbia, and the U.S. Virgin Islands have enacted a form of UETA.[62]

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.[63] 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.[64]

Congress responded by passing ESIGN, which, while mirroring UETA in many ways diverged in some provisions, including consumer consent requirements.[65] However, Congress included a pre-emption provision that gives states the option between ESIGN compliance or UETA adoption.[66] 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. [67] This reflected the desire that states either follow ESIGN or adopt UETA and displace ESIGN. [68] In this way, the preemption provision ensures that either ESIGN or UETA governs electronic transactions.

B. 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. [69] Second, both clarify that any law that requires a record to be in writing will be satisfied by an electronic record. [70] Finally, an electronic signature is held to be the equivalent of a written signature for any law that requires a signature. [71] 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." [72] ESIGN and UETA also have sections relating to the retention and accessibility of any electronic records. [73] Both acts require that an electronic record be producible and must accurately reflect the final form that the parties agreed upon. [74]

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. [75] 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. [76] 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. Simply put, asymmetric key encryption falls squarely within the both the language and intent of ESIGN and UETA as an "electronic signature."

As noted above, 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 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." [77] 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. [78] 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. [79] 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.[80] 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.[81] 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.[82] 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, as it would require cryptographic hacking that is only available to nation-state actors. 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 unlike in cases where someone's bitcoin wallet key is stolen to transfer funds, the benefits of stealing the key for an insurance contract or other type of blockchain-based smart contracts are much less obvious. 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, as fewer parties would be willing to go to court to contest that they signed a contract, as the evidence would be difficult to overcome.

Part III: Smart Contracts, Parametric Insurance, and the Smart Grid

Blockchain-based smart contracts have the potential to benefit the insurance and energy sectors by streamlining current activities and opening new markets for products. Both the insurance and energy sectors can take advantage of blockchain to digitize and streamline administration of existing processes and utilize the technology to offer new products and services where transparency, trust, and simplicity offer value. In the insurance industry, many of the most common forms of contracts can be reduced to simple "if-then" statements and digitized as blockchain-based smart contracts. Digitizing the administration of existing policies would reduce the cost of administering these products; using basic parameters for policy payout could leverage blockchain-based smart contracts' ability to easily administer "if-then" transactional relationships. In the energy industry, blockchain-based smart contracts can enable smart grids, microgrids, and other types of innovative grid management technologies by both providing the mechanism for automating value transmission and the means to streamline transaction administration. Blockchain's trust environment for transactions can also open new markets for innovative methods of service provision and payment for service. As such, both the insurance and energy industries provide real-world use cases to demonstrate the value of blockchain-based smart contract technology.

Insurance

Basic insurance contracts can often be boiled down to an agreement to make payment upon the occurrence of a discrete event. However, administration of even apparently straightforward insurance policies can become complex. Claims adjusters are needed to assess a claim and its validity. If parties later disagree about the interpretation of the terms, or the parties relied on representations outside of the policy, disagreements can arise. Parties are often mistrustful of one another even in the most cordial customer-service environment because of the potential for fraud, abuse, or denial of claims. In either event, insurance companies incur costs administering even the simplest of contracts, and those costs are often passed along to consumers in the form of higher premiums.

Blockchain-based smart contracts can avoid many of these problems. They can be structured to reflect the basic "if-then" relationship of many basic insurance policies. Through the use of event monitoring functions, such as oracles, payments can be automatically triggered based on objective validation of specified events. Construction of blockchain-based smart contracts requires the parties to precisely define the terms of the policy so that those terms can be executed by a digital protocol, since the protocol can be programmed to execute only explicit policy terms. Moreover, by overcoming challenges of trust and providing transparency, new types of policies for different or underserved populations can be structured and utilized.

A. Efficiency Gains in Current Insurance Contracts: Life Insurance and Final Expense Policies

Some of the simplest "if-then" types of insurance policies are individual life insurance and final expense policies. Life insurance contracts pay out upon the policyholder's death. Although this process is normally easy for the survivors to carry out, usually requiring the presentation of a death certificate or other proof of loss and a beneficiary form, problems can arise in multiple ways. For example, the policyholder may hold multiple life insurance policies, the beneficiary may not know about the policy, or the beneficiary may misplace the paperwork for the policy.[83] As a result, inefficiencies and increased administration costs can arise without any malfeasance or ill-will from any party.

Blockchain-based smart contracts can remedy many of these problems. For example, rather than maintaining only a written insurance contract, a blockchain-based smart contract is digitally instantiated and recorded to the blockchain's immutable ledger. Rather than relying upon the policyholder to retain the policy (making the policy subject to loss through misplacement or destruction by fire, flood, or similar occurrences), the policy would be recorded on the blockchain and its terms would be available at any time for the insurer, the policyholder, and the beneficiary to review. Rather than relying upon a beneficiary to notify the insurance company, a blockchain-based smart contract can be constructed to rely on oracles set to monitor specific sources of information about individual deaths. The transparency of the blockchain and the fact that its rules are not administered by any single participant in the process can allow purchasers to rely on digital instantiation and administration.

Digitization has already enabled portions of this process. The United States government maintains the Social Security Death Master File, which tracks when a person with a Social Security number dies.[84] Although this is not a perfect record and has in many instances been subject to legitimate criticism for its accuracy,[85] an oracle could monitor this file for policyholders, and upon the death of a policyholder the oracle could trigger the potential execution of the blockchain-based smart contract. Currently, the Master File is only updated once a week and a person's death must be reported to the Social Security Administration for it to be filed.[86] For that reason, oracles could also monitor other digitally-available sources of information, such as social media, in order to provide further assurances before the final execution of the contract.[87] Indeed, some organizations are already experimenting with peer-to-peer unemployment insurance smart contracts based on LinkedIn data.[88]

A similar application for blockchain-based smart contracts in insurance is final expenses insurance. Final expenses insurance is a form of insurance where a fixed sum is paid out upon a person's death to help cover funeral costs.[89] For some cultures, it is essential to have a proper funeral or perform funeral traditions.[90] However, families are often unable to pay for an unexpected funeral or even the funeral of an elderly family member. A blockchain-based smart contract could be set up using the same sources as a life insurance smart contract and perform the same function. Indeed, contracts could even be purchased by family members in other countries, with agreed-upon oracles and specified mechanisms of digital payment, such as direct payment to funeral providers, rather than reliance upon local reporting and paper checks.

B. New Models of Insurance: Parametric Insurance

Life insurance and final expense insurance are good examples of simple "if-then" arrangements that can be digitized into blockchain-based smart contracts in relatively straightforward ways. But could other types of insurance that are currently reliant on more subjective factors be restructured into products with more firmly defined parameters, enabling their digitization and administration through blockchain's transparent processes? Parametric insurance policies offer such potential. By pairing parametric insurance with blockchain-based smart contracts, insurers can reinvent the manner in which classes of insurance are offered.

Parametric insurance is a form of insurance where the payouts are determined not through a claims adjuster surveying the damage, but based on objective measures, such as the magnitude of a weather event.[91] It is most often used for insurance for natural catastrophes, such as tornadoes or hurricanes, where individualized policies based on specific damage would be difficult and costly to administer but a standardized payout based on proxies, such as the severity of the storm, would suffice.[92] Parametric insurance is preferable to other forms of insurance when a quick payout is necessary, such as when a country suffers a hurricane and needs to quickly obtain money to begin rebuilding and pay emergency workers.[93] Parametric insurance can lower the time of payment from months to two weeks, which can help jumpstart the rebuilding process.[94]

The key to parametric insurance is finding objective indicators that can serve as an effective proxy for the type of loss being covered. The benefit to doing so is that once effective proxies are identified, policies that would need to be adjusted qualitatively could instead be reduced to simpler "if-then" statements. For example, by relying upon objective markers, such as storm intensity, wind speed, or amount of rain, there is no need for individualized adjustment of claims. After a hurricane damages an area, an oracle can pull data from a third-party site, such as the National Weather Service, to determine objective measures, such as the strength of the storm, and then make a payment based on that data. While individual losses may be greater or less than the specified payment amount, the insurer gains certainty in loss forecasting and the policyholder gains speed in payment. Both parties benefit from the automation of the process and the reduction in frictional costs.

Parameterizing current forms of insurance based on proxies for loss and coding these policies onto blockchain-based smart contracts can fundamentally alter insurance offerings by (1) lowering transactional costs of simple policies to allow for lower-premium policies to be profitably administered and (2) opening new markets for insurance products since locally-based claims adjustors or other local trusted agents would no longer be necessary to effectively administer the policy. Although some costs are difficult to manage, studies have found that for property and casualty insurance, management and contract administration is the largest driver of cost variance.[95] Indeed, for property and casualty insurance, one study concluded that over eighty percent of the cost variance was attributed to management factors, not to the underlying product.[96] It is estimated that improving IT efforts alone could reduce costs by twenty to forty percent, with business complexity and performance management being other large drivers of cost variance.[97]

Moving to parametric blockchain-based smart contracts has the benefit of addressing IT improvement, business complexity, and performance management, while gaining transparency and trust. Blockchain technology can be implemented without having to discard current IT systems, as a blockchain-based platform can be added on top of an existing IT system and, indeed, is commercially available through several cloud services providers.[98] Parameterizing current policy structures drastically reduces business complexity, and its standardization of payouts and parameters allows for much more bounded modeling of potential loss events and amounts. Finally, blockchain-based smart contracts can be administered through oracles and monitored in real-time through analytic software examining the permanent blockchain record of transactions and loss occurrences, creating incentives both for parameterization and for reducing such policies to blockchain-based smart contracts. Fewer local agents would be necessary, and the use of oracles could replace the need to rely on the reports of adjusters on the ground.

As a result of the reduction in frictional costs, policies that were previously unprofitable because of low margins—due to the low premiums or high administration costs—could become profitable areas for new products. For example, companies could profitably insure extremely low premium and low payout events through no-fault parametric policies, where the payouts are determined based on readings from sensors installed in the cars about damage to the car, pattern of driving before the incident, violation of local traffic laws, or other factors.[99] Homeowners could have parametric insurance for incidents such as fires in their homes where a smart fire alarm and smart home sensors could identify the source of a fire, the resulting damage, and potentially its cause.

Moreover, the agricultural industry lends itself to the use of parametric, blockchain-based smart contract insurance. Touting the numerous potential benefits of parametric insurance to improve the welfare of smallholder farmers, increase resilience, and eliminate the need to verify losses, numerous organizations have piloted index insurance programs all over the world, particularly in developing countries.[100] However, the ability to reach smallholder farmers to make sure they can access and understand the insurance contracts currently limits scalability.[101] Rural areas with poor infrastructure may be hard to reach with traditional methods.

The ability to market and administer blockchain-based smart contract-enabled parametric insurance policies solely through internet-connected smartphones can aid in reaching underserved populations. For example, a smartphone-based system, potentially modeled after Kenya's M-Pesa,[102] could be a good solution. M-Pesa is a mobile payment system that allows people to send and receive money using their cellphone.[103] Since 2007, the technology has taken off with at least one individual in ninety-six percent of Kenyan households using it.[104] Indeed, seventy-five percent of the unbanked population in Kenya uses M-Pesa.[105] Elsewhere in Africa, BitPesa is using the Bitcoin blockchain to bring the M-Pesa model to other African countries and to cross-border transactions.

In sum, parametric, blockchain-based smart contracts represent not only an opportunity to digitize existing insurance products to realize efficiencies, but also open potentially untapped markets for insurance products using the benefits of newly-developed technology.

C. Smart Contracts, Insurance, UETA, and ESIGN

As noted above, we argue that blockchain-based smart contracts are enforceable under UETA and ESIGN. Specifically with respect to insurance contracts, however, these types of digital contracts are also the exact types of contracts that Congress wanted to protect under ESIGN. Insurance contracts are specifically included in the statute.[106] ESIGN, as part of its consumer protection provisions, prohibits the cancellation of life insurance policies through electronic means.[107] This protection reflects the special status of life insurance as providing for one's family after death, which has led states to protect life insurance proceeds in other ways.[108] UETA does not have a similar protection, but many states have implemented similar exemptions.[109] These limitations restrict the kinds of smart contracts that can be created for insurance products.

In order to take advantage of UETA and ESIGN, a blockchain-based smart contract for life insurance would not be able to cancel a policyholder's policy upon non-payment of the premium. Instead, the cancellation notice would need to be sent via physical form. Cancellation of blockchain-based smart contract-driven life insurance policies for non-payment may be an area for further development of legal guidance under UETA and ESIGN. In addition, smart contracts need to be worded carefully to ensure that policyholders do not use them as a substitute for a will, as ESIGN and UETA would not ensure that they are valid.

Smart Contracts and the Energy Industry

The energy industry is actively examining new models and mechanisms for delivering service to customers. Likewise, customers themselves are looking for new ways to purchase energy and to understand the origins of the energy they purchase. Blockchain-based smart contracts can help accelerate two developments in the energy industry: (1) smart meters; and (2) microgrids. Blockchain-based smart contracts can provide a new, more secure basis for smart meters and, in fact, can take advantage of blockchain's currency foundations to automate payments as well. Blockchain-based smart contracts are already enabling microgrids, and these initial efforts can point the way to broader adoption. Blockchain-based smart contracts can provide the tool to give both utilities and customers the levels of efficiency and effectiveness that both strive for, while delivering both the consumer protections and individual choice that stakeholders often advocate.

A. Smart Meters

Retail energy provides power to customers through energy lines. The electric utility tracks a customer's power consumption through a meter installed at the customer's home. At the end of the billing cycle, a customer is sent a bill for their past month's consumption.

Although this process is well understood by all parties involved, it has several drawbacks. First, by receiving a bill only once a month, it is difficult for customers to obtain immediate feedback on their energy usage. On a hot day, a customer may know that their usage will be higher, but they would not have a way of knowing exactly how much more energy they used that day compared to a regular day. For instance, they may know that keeping the house at 73 degrees will be expensive but not how much more expensive relative to keeping it at 75 degrees, which limits the ability of a household to adjust its usage on a less-than-monthly basis. If a homeowner wants to balance their comfort with keeping heating and cooling costs down, having access to this more granular level of detail will enable them make the best decision. Second, the process relies on customers being able to provide forms of identification and credit, which may be difficult for certain populations, like students and households without bank accounts. Many utilities require either a Social Security number or two forms of identification, including one with a photo. [110] Even if the potential customers do have those forms of identification, they may lack access to banks or credit cards that a utility requires. [111]

In response, some utility companies have begun to use smart meters, which are electrical meters that wirelessly send meter readings to the utility company. This allows the company to provide a more accurate and up-to-date bill while also freeing the company from needing to send inspectors out every month to read the meters. [112]

Smart meters can go a step further, however, to allow customers to pay as they go rather than rely on monthly assessments and the credit requirements. For example, Arizona's Salt River Project Agricultural Improvement and Power District ("SRP") implemented a pay as you go smart meter system, M-Power, which is currently one of the largest pre-paid energy programs in the United States. [113] Under M-Power, SRP installs smart meters in customers' homes and allows them to use pre-paid smart cards to purchase energy. These cards can be re-loaded at pay centers across the Phoenix metro area, which includes centers that are open 24 hours a day. [114] This system gives customers more control and flexibility over their energy bill, which is particularly beneficial for those with tight budgets, such as lower-income families or students. [115] Customers are also more aware of their energy usage, resulting in a twelve percent reduction in electricity use of M-Power customers. [116] With high satisfaction ratings, [117] SRP's customer base has also expanded from those needing more flexibility than a monthly electricity bill to include customers interested in measuring their energy use or wanting to reduce their energy use. [118]

Blockchain-based smart contracts could build further on the pay-as-you-go smart meter concept. For example, blockchain-based smart contracts can resolve some security concerns and allow for quicker payments. A recent report noted that smart-meters are woefully insecure, using outdated encryption protocols that can be easily brute-forced. [119] Some customers are also unable to reload their payment cards without visiting a separate payment machine, which can pose a problem if their energy runs out in the middle of the night and no pay centers are open. Finally, some consumers have protested that smart meters inaccurately measure their consumption and overcharge them. [120] By contrast, blockchain-based device authentication tools can augment the security of smart meters on a blockchain-based system. [121]

Blockchain-based smart contracts can also enhance payment processes for smart meters. Instead of relying upon payment cards that must be reloaded at a separate location, with blockchain-based smart contracts paired with smart meters, customers can arrange payments on their phones using blockchain-based smart contracts that execute when their remaining electrical power drops below a certain amount of time left. This makes it easier for customers to pay than the current system, which often requires going to a separate physical location to add to one's balance. Blockchain-based smart contracts could also be structured so that when an external weather reporting site indicates that the next week will be particularly cold or hot, the contract would automatically add more money to the consumer's balance to account for the expected higher usage. For some users, the assurance of knowing that they will not need to frantically add to their balance during the middle of a snowstorm or heat wave is worth paying earlier than necessary. The consumer would also benefit from having multiple smart contracts execute during what would have been a traditional monthly billing cycle. The consumer would have more immediate feedback about their energy usage and could adjust in real-time or based on pre-programmed parameters if necessary.

As noted above, blockchain technology also offers benefits of greater transparency for all participants, as well as a greater sense that rules cannot be changed unilaterally. As a result, a blockchain solution can address questions concerning overbilling. With a blockchain-based system, consumers would have direct access to an immutable record of their usage, which could be compared to historical usage or the average usage of neighbors. A user who suspects they were either overcharged or perhaps had their smart meter hacked would be able to compare their usage on an extremely granular level to the usage of their neighbors to demonstrate errors. These benefits may allow companies to reach new markets of people looking for more flexibility or who have difficulty with the traditional requirements.

B. Microgrids

Microgrids are another area of innovation in the electric industry. In the United States, the majority of people receive their electricity from coal and natural gas facilities. [122] These facilities generate power at a central location, which is then transmitted over power lines to the end user. Although this is the dominant model for delivering power in the United States, this model presents specific risks.

For example, centralized power production creates a risk that if a plant goes offline, customers will suffer substantial loss of service. Hurricane Sandy demonstrated this problem in dramatic fashion. The hurricane left 7.9 million people without power in the Mid-Atlantic and New England areas in the immediate wake of landfall. [123] Even a month later, one percent of Jersey Central Power & Light customers remained without power. [124] The crippling effects of the storm demonstrated that an electrical grid relying upon a few central power plants could collapse quickly and need a lengthy rebuild. The fact that multiple storms in the previous year had knocked power out to millions of people on the Eastern Seaboard further confirmed that the electrical grid was vulnerable. [125] For these and other reasons, the centralized grid model has been criticized in recent reports as being outdated and in need of serious upgrade. [126]

Microgrids are a potential supplement to centralized grid systems, but may eventually replace them altogether. Rather than rely exclusively upon a power plant that produces electricity for a region, a microgrid allows residents in the area to better manage local usage and even generate and sell power through solar panels or other alternative energy methods. [127] The residents can use the microgrid to power their own homes or businesses, supplement their power needs from the larger grid—and if they generate extraneous power, residents can sell it either to their neighbors or back to the larger grid. [128] Microgrids provide a backup system in case a storm or terror event disables the centralized grid. In fact, several microgrid participants cited access to a reliable backup as part of the reason that they joined the project. [129] Microgrids may even extend power access to rural and tribal communities. [130]

Blockchain technology is beginning to be deployed in the United States to facilitate microgrids. [131] The most successful example so far is the Park Slope microgrid in Brooklyn, New York, with over 130 buildings participating. [132] Although currently limited in scope, the ultimate goal is to use blockchain-based smart contracts to allow buildings that produce extra energy to sell that energy in an automated fashion to other residents on the microgrid. [133] Blockchain-based smart contracts would be set up in such a way that when one user produces excess energy, it is automatically sold to another user in the neighborhood, which allows the neighborhood to lessen the amount of energy it draws from the central grid. Facilitating the sale of excess energy produced by one building to a building in need of energy helps reduce the overall strain on the grid, thereby preventing brownouts during times of high-energy consumption. The Park Slope microgrid has already led to reduced energy usage, as well as facilitating a better understanding amongst consumers regarding where the energy originates and how it is made. [134] The emphasis on buying energy as needed forces customers to confront their energy usage and re-evaluate how much they are using. [135]

Adopting blockchain technology in the energy industry poses its own challenges. Strict industry regulation and monopolies make it difficult to implement new technologies even with their likely benefits. For example, as a political subdivision of the state of Arizona, SRP is under different regulations from the Arizona Corporation Commission ("ACC") than a standard utility company. [136] This regulatory freedom allowed SRP to test and implement its pay-as-you-go smart meters. In this way, co-ops are also strong candidates to begin experimenting with and adopting blockchain-based smart contract technology, in a manner that can ultimately benefit the entire industry.

Conclusion

With all of the hype surrounding blockchain-based smart contracts, it is important to focus on the use cases that are both viable and valuable. Blockchain-based smart contracts should be seen as a legally binding statement under UETA and ESIGN and, therefore, available for innovation now. Moreover, the benefits of blockchain-based smart contracts are clear. Blockchain-based smart contracts provide security and resilience, an immutable transaction history, and the ability to enable micropayments, micro-transactions, and automation in an effective and profitable manner.

The insurance industry could greatly benefit from blockchain-based smart contracts, particularly for contracts that can be easily automated or broken down into "if-then" statements. This would allow the industry to reach new markets while also solving some existing problems. Blockchain-based smart contracts would reduce the need for intermediaries, copious amounts of paperwork, and cases of underpayment while simultaneously increasing efficiency and decreasing payout time. Parametric insurance may prove to be the best application of blockchain-based smart contracts in the insurance industry, leading to lower transactional and administrative costs and reducing the need for claims adjustors, which will in turn reduce premiums. With 2.5 billion unbanked people in the world, a new payment system using blockchain could open up a huge new market of potential customers.

Another promising application is in the energy industry. Blockchain-based smart contracts could increase the efficiency of payment systems and energy transfer while also improving security and resilience. Customers would also have more freedom and information on their energy usage and costs using blockchain-based smart contracts. Microgrids will increase resilience of the energy system, which may become more essential with severe weather patterns or potential terrorist attacks. Blockchain-based smart contracts will also allow people to easily sell or buy more energy depending on their usage at any given time. With fewer regulatory barriers, co-ops may be the best starting place for implementing these new applications within the energy sector, to the overall benefit of the energy industry as it can observe these experiments and take advantage of the technology as it matures.

In sum, rather than simply a futuristic science project, blockchain-based smart contracts are real, enforceable under existing law, and able to offer real benefits across a variety of industries.

Alan Cohn, Travis West, and Chelsea Parker

*Alan Cohn is Of Counsel at Steptoe & Johnson LLP and Adjunct Professor, Georgetown University Law Center; he is also an advisor to several blockchain technology companies. Travis West is an Associate at Steptoe & Johnson LLP, Harvard Law, J.D. 2016, and Chelsea Parker is a Project Assistant at Steptoe & Johnson LLP, Princeton University, B.A., 2014. Cohn is co-chair, and West and Parker are members, of Steptoe's Blockchain and Digital Currency Practice.

Share this:

Related

Blockchain Technology Impact on Energy Market Transformation: Secured Distributed Energy Transactions in the Cloud
April 2017
In "Legal News"

The Law and Legality of Smart Contracts
April 2017
In "Articles"

"Smart Contracts": A Smart Way to Automate Performance
April 2017
In "FintechExplainer"

Articles
Vol. I, Issue II (2017)
ZZZ-Featured Article
Tags: Blockchain, Fintech, Smart Contracts

Privacy | Alumni