2019

Crypto-Concerns: A Cyberskeptic Looks for Weak Links in the Blockchain

Becky L. Jacobs

A CYBER-SKEPTIC'S CONCERNS ABOUT THE STATE OF LEX CRYPTOGRAPHIA: A RESPONSE TO MARCIA WELDON'S "BEYOND BITCOIN: LEVERAGING BLOCKCHAIN TO BENEFIT BUSINESS AND SOCIETY"

Becky L. Jacobs *

In her article, "*Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society*" Professor Weldon explores the potential of blockchain technology to transform corporate governance and risk management and to promote the principles of transparency that animate various mandatory disclosure regimes.[1]

I too am very excited by blockchain's potential to revolutionize and make more transparent many business practices, but I also have some, pun intended, crypto-concerns. I admit that these concerns are based upon

* Waller Lansden Distinguished Professor of Law, University of Tennessee College of Law. Email: jacobs@utk.edu. I want to acknowledge my wonderful colleagues, Joan Heminway and George Kuney, who have a talent for organizing thought-provoking symposia and who allow me to participate, and to William A. Beasley and Adelina S. Keenan, the *Transactions: The Tennessee Journal of Business Law* editors who had to contend with dramatic weather and professionals to make the event possible and enjoyable. Thanks also to all of the Business Law Prof Bloggers who attended and stimulated the intellect, particularly Marcia Narine Weldon, whose presentations and scholarship are always enlightening, entertaining and inspiring.

[1] Marcia Weldon, *Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society,* 20 TENN. J. BUS. L. 837 (2019). Professor Weldon's comments focus on consortium (permissioned) and private distributed ledger technologies ("DLTs"); my thoughts will be more applicable to public (permission-less) DLTs. These terms refer to the three operating blockchain platforms: (1) public, permission-less; (2) consortium, permissioned, and (3) private. Anyone can participate in a public DLT through the consensus process, i.e., Ethereum. Access to consortium, permissioned blockchains is limited by the determined multiple organizations that manage it, as is true with a private blockchain that is managed by one organization with full control. *See* Nabil El Ioini & Claus Pahl, *A Review of Distributed Ledger Technologies*, OTM CONFEDERATED INTERNATIONAL CONFERENCES, ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS (Springer, Cham, 2018), https://tinyurl.com/yacp7bh9. Some contend that "private" blockchains really are repackaged shared databases as the blockchain's defining innovation was its proof-of-work consensus mechanism. *See, e.g.*, Arvind Narayanan, *"Private blockchain" is Just a Confusing Name for a Shared Database*, Freedom to Tinker (Nov. 2018), https://freedom-to-tinker.com/2015/09/18/private-blockchain-is-just-a-confusing-name-for-a-shared-database/.

my natural skepticism for anything that is alleged to be foolproof. They also, however, are based upon our very real experience with the internet, which makes it clear that we need to make certain that the technology is truly ready to adequately and securely execute the tasks that we are being told it can accomplish and that there is a legal framework in place to manage the inevitable disputes that arise from its use. Anyone who has had their email hacked or has been impacted by identity theft through a database breach should be similarly cautious.

Blockchain technology interacts with the law in a number of contexts, corporate governance being one (as well as copyright and other IP, tax, antitrust, securities regulation, banking, criminal, corporate, maritime, insurance, and on and on), and it raises questions about the very nature of what blockchain technology can represent, such as Bitcoin, zencash, Ether, or other cryptocurrencies or currency-related products. Are these currencies "property" as traditionally conceptualized?[2] Are they legally-defined securities, as another article in this symposium explores? Scholars, lawyers, and policy makers are grappling very publicly with these questions alongside IT professionals. This intense interest is obvious; if you search Google with the term "Blockchain" returns "About 219,000,000 results (0.39 seconds)[.]" There also are hundreds of scholarly articles that discuss blockchain questions on research networks.

I will focus on just a few concerns. The first is on the "smart contracting" aspect of blockchain technology, and the second pertains to its current negative environmental impact. My concluding remarks will touch upon the concept of "transparency" in the promotion of blockchain technology in the legal context.

[2] Just FYI: In the U.S., cryptocurrency is treated as property for federal tax purposes. Internal Revenue Service, *IRS Virutal Currency Guidance: Virtual Currency is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply*, IR-2014-36 (Mar. 25, 2014). For a complete survey of global regulation of virtual currencies, see U.S. LAW LIBRARY OF CONGRESS, GLOBAL LEGAL RESEARCH CENTER, REGULATION OF CRYPTOCURRENCY AROUND THE WORLD (June 2018), https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

Smart Contracts:[3]

I want to frame my comments regarding smart contracts with Lawrence Lessig's pronouncement that "code is law."[4] His words were very prescient in 1996:

> [A regulator] in cyberspace need only change the code-the software that defines the terms upon which the individual gains access to the system, or uses assets on the system. If she wants to limit trespass on a system, she need not rely simply on a law against trespass; she can implement a system of passwords. . . . [T]here is a code (as in software) to assure what the code (as in law) demands. . . . Code is an efficient means of regulation. . . . One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else. There is no choice about whether to yield to the demand for a password; one complies if one wants to enter the system. In the well implemented system, there is no civil disobedience. Law as code is a start to the perfect technology of justice.[5]

In 2006, he revisited the topic and found that "[c]ode can, and increasingly will, displace law"[6] and shifts "effective regulatory power from law to code, from sovereigns to software."[7]

---

[3] This essay does not provide a legal analysis of the status of cryptocurrencies or their initial offerings ("ICOs"). Also, for purposes of this article, I proceed on the assumption that smart contract are "contracts" in a theoretical sense. Several commenters have raised this issue: "Smart contracts are designed to eliminate the need for legal enforcement. The central feature of a smart contract—what supposedly makes them smart—is that legal enforcement will not be necessary or even possible. In a very real way, smart contracts are not intended to be legally enforceable." Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 339 (2017). Tangentially, others contend that the term "'smart contract' is itself imperfect. A smart contract is neither smart, nor is it necessarily a contract. A smart contract is computer code programmed to execute transactions based on pre-defined conditions. . . . Because a smart contract is computer code, a smart contract may represent all, part, or none of a valid legal contract. . . . Thus, smart contracts are the programmatic means by which some or all of the terms of the legal contract are performed." Digital Chamber Of Commerce, *"Smart Contracts" Legal Primer - Why Smart Contracts Are Valid Under Existing Law And Do Not Require Additional Authorization To Be Enforceable* 1–2 (Jan. 2018).

[4] Lawrence Lessig, Code Version 2.0 at 5 (2d ed. 2007).

[5] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 (1996).

[6] Lessig, *supra* note 4, at 175.

[7] Lawrence Lessig, Code and Other Laws of Cyberspace 206 (1999).

Smart contracts are basically these cryptographic codes as law, capable of facilitating, executing, and enforcing the negotiation or performance of an agreement using blockchain technology. Because they are designed and implemented within blockchains, they inherit some of its properties, i.e., they are validated by and exist within the distributed ledger system of the chain, and, as such, they are theoretically difficult for an attacker, or one of the parties, to hack or alter in bad faith.

Nick Szabo, who some speculate may be the elusive creator of bitcoin, Satoshi Nakamoto, coined the term "smart contract." This is how he describes the concept in his original paper on the topic:

> A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, . . . dispense[s] change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.[8]

If anyone has lost money in a vending machine, I think you might see where my technological concerns might be given Szabo's simple analogy. If the technology does not work, well, your options for cure are limited in both instances: shaking, kicking, cursing.

I am not being overly captious or a doom-monger. As William L. Fitts also will discuss, in 2016, a hacker "stole" $50 million from the original Decentralized Autonomous Organization ("DAO") based on the Ethereum blockchain.[9] Another example: in November 2017, a bug in Parity, an Ethereum wallet for cryptocurrency, resulted in more than $150

---

[8] Nick Szabo, *Formalizing and Securing Relationships on Public Networks* (1997), https://ojphi.org/ojs/index.php/fm/article/view/548/469.

[9] *See* QUINN DUPONT, EXPERIMENTS IN ALGORITHMIC GOVERNANCE: A HISTORY AND ETHNOGRAPHY OF 'THE DAO,' A FAILED DECENTRALIZED AUTONOMOUS ORGANIZATION 7 (Routledge ed. 2017).

million worth of Ether being permanently frozen.[10] A careless developer effectively destroyed a piece of Parity's code, rendering all of the wallets that were created after that piece of code's creation unusable.

Unfortunately, these two examples are not aberrations. A team of computer scientists from University College London analyzed a sample of nearly one million Ethereum smart contracts, flagging around 34,000 as vulnerable—including the one that led to the Parity fund freeze, or lock.[11] On a subset of 3,759 contracts that the team sampled for validation, it reproduced real exploits on a whopping 89% (yielding exploits for 3,686 contracts).[12]

Interestingly, the lead investigator in that study compared the team's work to interacting with a vending machine, as though the researchers randomly pushed buttons and recorded the conditions that made the machine act in unintended ways.[13] They found three primary vulnerabilities in the smart contracts that they analyzed:[14] (1) "Greedy" contracts that locked funds indefinitely, (2) "Prodigal" contracts that leaked funds carelessly to arbitrary users, or (3) "Suicidal" contracts that could be "killed" by any arbitrary account.[15] The team estimated that the maximum amount of Ether that could have been withdrawn from leaking and suicidal contracts was US$ 5.9 million.[16] It further approximated that US$ 7.5 million was locked in "dead" contracts on the blockchain, US$ 379,940 million of which had been sent *after* these contracts had been killed.[17]

---

[10] Stan Schroeder, *Wallet Bug Freezes More Than $150 Million Worth of Ethereum* (Nov. 8, 2017) https://mashable.com/2017/11/08/ethereum-parity-bug/#Hxi0yPyJ_mqE.

[11] IVICA NIKOLIC ET AL., FINDING THE GREEDY, PRODIGAL, AND SUICIDAL CONTRACTS AT SCALE 1–2 (Mar. 14, 2018) abs/1802.06038 (2018), arXiv:1802.06038, http://arxiv.org/abs/1802.06038.

[12] *Id.* at 1, 2, 10.

[13] Mike Orcutt, *Ethereum's Smart Contracts are Full of Holes*, MIT TECHNOLOGY REVIEW, Mar. 2018, at 1–2, https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/.

[14] NIKOLIC ET AL., *supra* note 11, at 2.

[15] *Id.* at 3-4.

[16] *Id.* at 13.

[17] *Id.*

This is not the only vulnerability to which blockchain smart contract technology is subject. While the structure of a distributed ledger is claimed to be virtually impossible to hack, the private keys required to access a blockchain can easily be stolen. If a hacker gains entry to the blockchain, they have access to the key holder's account and can "view"[18] all information on the ledger.

There is also the 51% attack problem. This can occur because an attacker or a group controlling 51% of the computing power on the network can interfere with the process of recording new blocks, theoretically allowing the attacker or group to monopolize the mining of new blocks.[19] The attackers also can send a transaction, then reverse it, making it appear as though they still possess the currency that they just spent, a vulnerability known as double-spending, the digital equivalent of counterfeiting.[20] At one time a theoretical risk, these attacks are becoming regular occurrences. At least five cryptocurrencies were hit with 51% attacks over the summer, resulting in losses of the equivalent of nearly $20 million dollars.[21]

These susceptibilities illustrate the technical vulnerabilities to which smart contracts are subject, but there also are substantive and structural concerns, such as how the lex cryptographia or cyber law

---

[18] One might question the applicability of the use of the term "view," a concept that I will explore briefly in the conclusion to this essay.

[19] *See, e.g.*, Lawrence Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?,* 20 RICH. J.L. & TECH. 13, 1 (2014). Some contend that the threshold for such an attack is substantially lower than 50% and, due to the danger that so-called selfish mining poses to the Bitcoin ecosystem, propose thresholds of no more than 25-33%. *See* Ittay Eyal & Emin Gün Sirer, *Majority is not Enough: Bitcoin Mining is Vulnerable*, 61 COMM. OF ACM 95, 102 (2018).

[20] *Id.*

[21] David Canellis, *Cryptocurrency Hackers Earned $20 Million in 2018 with So-Called 51% Attacks*, BUSINESS INSIDER (Oct. 24, 2018), https://www.businessinsider.com/cryptocurrency-hackers-earned-20-million-with-51-percent-attacks-in-2018-2018-10?r=UK&IR=T. *See also* Alyssa Hertig, *Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*, COINDESK (June 9, 2018), https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/. There are other malicious bugs, such as one found in the blockchain associated with the cryptocurrency "zcoin" that would allow users to print unlimited zcoin. Rob Price, *A Single Typo Let Hackers Steal $400,000 from a Bitcoin Rival*, BUSINESS INSIDER (Feb. 20, 2017), https://www.businessinsider.com/typo-bitcoin-rival-zcoin-attacker-steals-400000-2017-2?r=UK.

addresses smart contracts, if it does, and how these contracts interact with off-line, or extranet, laws, particularly if disputes arise.

These are still very much unsettled questions, but technology development has not paused in order to resolve them. Sites utilizing distributed ledger technology have forged ahead with their own extralegal systems existing entirely in the digital environment. For example, OpenBazaar, an open source network much like eBay (but without the fees), offers multi-signature escrow for cryptocurrency payments as well as a "moderator" system to settle disputes.[22] The moderators are selected by the disputing parties in OpenBazaar's open marketplace.[23]

Other decentralized crypto-"courts" are evolving, including Kleros, a self-described "decision protocol for a multipurpose court system [and an] Ethereum autonomous organization that works as a decentralized third party to arbitrate disputes in every kind of contract, from very simple to highly complex ones."[24] Kleros is a fully-automated arbitration process, the integrity of which is designed upon game-theoretical economic incentives.[25] The Kleros platform has received even mainstream attention,[26] but there are other systems vying for the business of resolving smart contract disputes, such as JUR[27] and Sagewise.[28] Indeed, some providers of blockchain technologies such as the Aragon Network are offering "to act as . . . digital jurisdiction[s]," essentially replacing choice of law with choice of code and making national or transnational law redundant. If blockchain technologies contain alternate, digital

---

[22] List of features of Openbazaar, OPENBAZAAR, https://openbazaar.org/features/ (last visited Jan. 21, 2019).

[23] *Id.*

[24] Clement Lesaege & Federico Ast, *Kleros—Short Paper v 1.0.6*, KLEROS (Nov. 2018), https://kleros.io/assets/whitepaper.pdf.

[25] *Id.*

[26] *See, e.g.*, Jay Kim, *In The Future Blockchain Will Solve Most Real-World Problems—Even Arbitration*, FORBES (Apr. 4, 2018), https://www.forbes.com/sites/kimjay/2018/04/04/in-the-future-blockchain-will-solve-most-real-world-problems-even-arbitration/#41f42461bd2f. Guidelines to govern the creation, performance, and enforcement of smart contracts also are beginning to appear. JAMS, previously known as Judicial Arbitration and Mediation Services, Inc., is among the "first institutional ADR providers to create protocols supporting the use of ADR in disputes arising from blockchain activities, including smart contracts." Services implementing these services surely will follow.

[27] JUR, https://jur.io/ (last visited Jan. 21, 2019).

[28] SAGEWISE, https://www.sagewise.io/ (last visited Jan. 21, 2019).

mechanisms of contract enforcement, what, if any, are their jurisdictional boundaries?

In the event a dispute exits a URL and enters the IRL, does any law, and, if so, what law, applies? Consider, for example, a cross-border blockchain dispute involving cryptocurrency. The original paper on smart contracts in which Szabo sets forth his vision of a new contracting world contained numerous vague statements about "common law."

> Over many centuries of cultural evolution has emerged both the concept of contract and principles related to it**,** encoded into common law. Such evolved structures are often prohibitively costly to rederive. If we started from scratch, using reason and experience, it could take many centuries to redevelop sophisticated ideas like contract law and property rights that make the modern market work. But the digital revolution challenges us to develop new institutions in a much shorter period of time. By extracting from our current laws, procedures, and theories those principles which remain applicable in cyberspace, we can retain much of this deep tradition, and greatly shorten the time needed to develop useful digital institutions. Computers make possible the running of algorithms heretofore prohibitively costly, and networks the quicker transmission of larger and more sophisticated messages. Furthermore, computer scientists and cryptographers have recently discovered many new and quite interesting algorithms. Combining these messages and algorithms makes possible a wide variety of new protocols. These protocols, running on public networks such as the Internet, both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world.[29]

If one presumes that some sort of IRL legal regime applies, there is the possibility that the law of the algorithmic code may conflict with the real-world law. The most obvious IRL case is the conviction of Ross W. Ulbricht on charges of drug trafficking and other crimes related to his

[29] Szabo, *supra* note 8.

development and operation of the darknet illegal marketplace, the Silk Road.[30] Alternatively, those seeking to exploit blockchain vulnerabilities may raise the "code-as-law" defense as did the DAO hacker who "transferred" $50 million of Ether; the code defines legality.[31]

Even assuming legality, however, are parties even able to seek legal enforcement in brick and mortar courts if such conflicts arise? For some, the answer is an unqualified "yes." To this group, "smart contracts" are not necessarily contracts but rather are computer code programmed to execute *the terms* of a legal contract, and, as such, traditional legal analysis and existing laws are sufficient to respond to legal disputes arising from these types of agreements, regardless of their form.[32]

Where do parties turn, however, if they do not agree with or cannot find a favorable reception for that contention? Obviously, there currently is little-to-no regulatory oversight of, or authority over, blockchains. In fact, in blockchain transactions, as it is exceptionally difficult to even identify the parties to the transactions, it would be difficult to order enforcement extra-cryptographically.[33]

Some governments and standard-setting organizations are beginning to address these issues. Internationally, the International Standards Organization has established a technical committee, ISO/TC 307, to develop standards for blockchains in a number of key areas: reference architecture, taxonomy and ontology, use cases, security and privacy, identity and smart contracts.[34]

---

[30] United States v. Ulbricht, 858 F.3d 71, 82-83 (2d Cir. 2017), *cert. denied*, 138 S. Ct. 2708 (2018); *Cf.* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (Mar. 10, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

[31] *See* Dupont, *supra* note 9, at 10. *See also* Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1401 (2018).

[32] *See* Digital Chamber of Commerce, *supra* note 3, at 1–2.

[33] ANDREJ SAVIN, BLOCKCHAIN, DIGITAL TRANSFORMATION AND THE LAW: WHAT CAN WE LEARN FROM THE RECENT DEALS? 4 (2018), http://openarchive.cbs.dk/bitstream/handle/10398/9648/Savin_Blochain.pdf?sequence=1. A court order could, perhaps, be enforced with a new transaction in a chain, but that is not possible without an access key.

[34] *ISO/TC 307: Blockchain and Electronic Distributed Ledger Technologies*, INT'L ORG. STANDARDS, https://www.iso.org/committee/6266604.html (2016).

Regulatorily, there is significant interest in blockchain and smart contract technology at all levels of government, but there does not appear to be a formal, official regulatory response,[35] perhaps because of the lack of generally accepted standards in the still-emerging technology. There are some notable exceptions. China, for example, has been very active regarding blockchain governance,[36] i.e., the Cyberspace Administration of China has published draft rules to regulate blockchain projects.[37] French legislators also have introduced blockchain-specific legislation pertaining to the use of blockchain for recording financial and other instruments and for improving their ownership authentication.[38] While other nations have announced "sandboxes," or legally-approved experiments with blockchain, or plans to develop legislation, no other laws[39] appear to have been enacted, nor does there appear to be much interest in developing an international convention or treaty on blockchain issues.

Focused more specifically on smart contracts, lawmakers in Monaco recently approved a bill creating a legal foundation for smart contracts, and several nations are engaged in activity pertaining to non-cryptocurrency-related smart contracts.[40] In the U.S., the action is at the

---

[35] This excludes activity related to cryptocurrency. *See generally, e.g.*, U.S. LAW LIBRARY OF CONGRESS, GLOBAL LEGAL RESEARCH CENTER, *supra* note 2.

[36] China presents a fascinating political case vis-à-vis blockchain technology. As one journalist wrote, "the Chinese government is seeking to "have its cake and eat it too" when it comes to crypto assets and blockchain technology. The simple phrase "blockchain not Bitcoin" has become the country's defining strategy when it comes to the space, and the difference in approaches that the government has taken regarding closed v. open ledgers and assets is a study in contrast." Steven Ehrlich, *Making Sense Of China's Grand Blockchain Strategy*, FORBES, Sep 17, 2018, https://www.forbes.com/sites/stevenehrlich/2018/09/17/making-sense-of-chinas-grand-blockchain-strategy/. China "plans to aggressively invest in the development of fintech and blockchain technology . . . [while at] the same time, the CPC has been overtly hostile to any and all activities related to crypto assets[, banning] all ICOs in the country [and] blocking crypto-related accounts." *Id.*

[37] Samuel Haig, *News-China Seeks Public Feedback on Draft DLT Regulations*, BITCOIN.COM (Oct. 2018), https://news.bitcoin.com/china-feedback-dlt-regulations/.

[38] *See* Stéphane Blemus, *Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide*, REVUE TRIMESTRIELLE DE DROIT FINANCIER (CORP. FIN. & CAPITAL MKTS L.R., RTDF N°4-2017) 11-12 (2017), https://dx.doi.org/10.2139/ssrn.3080639.

[39] Several U.S. states have passed blockchain-related legislation, including Nevada's 2017 law that made it the first U.S. state to ban local governments from taxing blockchain use. NEV. REV. STAT. §§ 244.3535, 268.0979 (2017).

[40] FLORIAN MÖSLEIN, CONFLICTS OF LAWS AND CODES: DEFINING THE BOUNDARIES

state level. Tennessee, for example, passed legislation in 2018 recognizing the legal authority to use blockchain technology and smart contracts for electronic transactions.[41] The legislation also includes a provision that "protects ownership rights of certain information secured by blockchain technology."[42] Arizona has similar legislation, enacted in 2017. [43]

In Vermont, a law enacted in May 2018 allows blockchain-based limited liability companies ("BBLLCs") to use blockchain technology for various aspects of corporate governance, including the use of smart contracts to administer the BBLLC's voting procedures.[44] This raises some very interesting questions about how well decentralized networks with governance structures encoded in software architecture fit within traditional legal schema for business associations.[45]

In addition to the uncertainty regarding their interaction with IRL legal systems, smart contracts also suffer from a fact of contractual life: ambiguity. Subjective contract determinants of quality, reasonableness, best efforts, buyer satisfaction, timeliness, force majeure, etc. plague their execution, too. Szabo's original article concedes this fact, and I quote, "[u]nlike most real-world contracts, protocols must be unambiguous and complete."[46] He appears, though, to think that most contract terms can be coded unambiguously, i.e., consider his rather offhand reference to the

---

OF DIGITAL JURISDICTIONS 8 (2018).

[41] *See, e.g.*, TENN. CODE ANN. §§ 47-10-201, 47-10-202 (2018).

[42] TENN. S.B.1662/H.B.1507 (Mar. 2018).

[43] *See, e.g.*, ARIZ. REV. STAT. ANN. §§ 44-1801, 44-7061 (2018).

[44] *See, e.g.*, VT. STAT. ANN. tit. 11, § 4175, et seq. (2018).

[45] While blockchain technologies are promoted as operating more democratically, there are significant regulatory and operational risks for decentralized networks. Traditional business associations are juristic personalities based upon legally mandated frameworks to which the encoded governance structures of decentralized autonomous organization with their multiple, geographically diverse, and anonymous stakeholders are not easily adapted. For a more detailed discussion of this topic, see Carla L. Reyes, Nizam Geslevich Packin, & Benjamin P. Edwards, *Distributed Governance*, 59 WM. & MARY L. REV. ONLINE 1 (2017). Despite this challenge, several states have enacted or are considering blockchain-related amendments to their corporate laws. Delaware, for example, amended its corporate law to allow maintenance of a distributed ledger of records administered by or on behalf of a corporation. Del. Code Ann. tit. 8, § 224 (West 2017).

[46] Szabo, *supra* note 8.

possibility that smart contract reifications could "account for hardship and operational exceptions."[47]

However, if an oracle creates a block that invokes a smart contract breach protocol for which the alleged breaching party has a valid excuse or defense, but one for which the code does NOT account, the very impregnability of a blockchain would appear to make it incredibly difficult to respond to problematic challenge-response algorithms.[48]

Environmental Impact

I could go on for pages about this, but let me just briefly mention my second concern, which is the environmental impact of blockchain technology. Putting aside environmental compliance, energy peer-to-peer microgrids, and the many other potential positive environmental issues which blockchain might address, the technology also has an immediate negative environmental impact as utilized by some applications.

The impact to which I refer is the energy intensity required by Bitcoin and several other cryptocurrencies that utilize proof of work mining processes to validate transactions.[49] Processing a Bitcoin transaction consumes an estimated 5,000 times as much energy as using a credit card, and it is estimated that Bitcoin mining, which requires energy-intensive server farms, consumes as much energy as was used by 159 of the world's nations.[50] This is particularly important because

---

[47] *Id.* (discussing the fiduciary duty of orders).

[48] The analysis has become more sophisticated with some suggesting that smart contracts can either outsource the legal assessment of ambiguities to an expert human oracle or "deviate from the law by replacing the rule with a simpler hard-and-fast rule." Eric Tjong Tjin Tai, *Force Majeure and Excuses in Smart Contracts* 12 (Tilburg Private Law, Working Paper No. 10, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3183637. While this second approach makes implementation and satisfaction of contracts an executable function, it merely "shift[s] the costs of contracting to the pre-contracting stage, as everything has to be drafted in the contract" before contract execution. *Id.* at 17–18.

[49] Saeed Elnaj, *The Problems With Bitcoin And The Future Of Blockchain*, FORBES (Mar. 29, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/the-problems-with-bitcoin-and-the-future-of-blockchain/#2488e90a68dc. Ethereum is another prominent cryptocurrency that makes use of proof of work. Lucy Berry, *Traditional Cryptocurrency Mining is Harmful for Environment*, HASHGAINS BLOG (Feb. 17, 2018), https://www.hashgains.com/blog/traditional-cryptocurrency-mining-harmful-environment/#.

[50] Bernard Marr, *The 5 Big Problems With Blockchain Everyone Should Be Aware Of*, FORBES (Feb. 19, 2018), https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-

cryptocurrency mining is expanding in countries like China, where 60% of Bitcoin mining takes place and where server farms are often powered by inefficient coal-fired plants.[51] As the process for validating transactions becomes more complicated, Bitcoin's power demand is only likely to increase, demanding as much electricity as the entire U.S. by 2019.[52] This is simply unacceptable, particularly given the availability of digital currencies, such as Ether and Ripple, that are processed differently.[53]

Transparency

Before I conclude, I want to briefly issue a warning about the "transparency" mantra that blockchain adherents chant to promote the technology. What does transparency mean in this context? On a blockchain, advocates repeatedly tell us, even although user identities are cryptographically concealed, "explorer" browsers display the contents of individual blocks and transactions, and transaction histories of public anonymous addresses.[54] This makes blockchain sound groundbreaking, but, as one report notes, "[f[ew people understand what it is, but Wall Street banks, IT organizations, and consultants are buzzing about blockchain technology."[55] Unless you read and write sophisticated programming languages such as C++, Java, Ruby, Simplicity, Python, and Solidity,[56] you are out of luck and will be wholly dependent upon coders for translation.

As those who do international work are well aware, translations are fraught with problems even when working with legal professionals under the very best of circumstances. Attempting to explain sophisticated contractual clauses to IT professionals who have not also had legal training

problems-with-blockchain-everyone-should-be-aware-of/#228a93ee1670.

51 DAVID REJESKI & LOVINIA REYNOLDS, BLOCKCHAIN SALVATION 3 (Envtl L. Inst. Policy Brief, June 2018), https://www.eli.org/sites/default/files/eli-pubs/policy-brief-14-web.pdf.

52 *Id.*

53 *See* Elnaj, *supra* note 49. "Ether, for example, uses the proof-of-stake concept, which is energy efficient, while the cryptocurrency ripple does not require mining." *Id.*

54 Blockchain Transparency Explained, Lisk (2018), https://lisk.io/academy/blockchain-basics/benefits-of-blockchain/blockchain-transparency-explained.

55 Research Briefs, *What Is Blockchain Technology?*, CBInsights (Sept. 11, 2018), https://www.cbinsights.com/research/what-is-blockchain-technology/.

56 Blockchain Coding: The Many different Languages You Need!, Blockgeeks, https://blockgeeks.com/guides/blockchain-coding/ (last visited Nov. 11, 2018).

in order to ensure accurate and precise autonomous execution certainly does not qualify for my "best of circumstances." One author predicts that "[f]raudulent and unconscionable contract terms, traditionally policed by courts, [will] likely proliferate as 'code-savvy parties' take advantage of the 'code-naive.'"[57] As with the predictions associated with AI, technologically -adept lawyers will survive and thrive in a blockchain prolific future; further segmentation vis-à-vis this technocratic class system may marginalize others.

Conclusion

That wraps up my very quick overview of the approximately 219,000,000 results from Google, even though it did take longer than 0.39 seconds. I will conclude by noting that businesses, and business lawyers, even those embracing new technologies, understand that complex business situations involve concepts and relationships that can be captured only imperfectly by heavily negotiated and carefully drafted contracts. Transactions and operations often require the kind of flexibility fundamentally at odds with algorithmically-constructed smart contracts, which, by their very nature, must be unambiguous. For such situations, the automatic execution of smart contracts is a software bug, not a feature.

Professor Weldon's recommendation that "boards put blockchain on their agendas to explore the impact the technology has on the business . . . [g]iven the increasingly widespread use of the technology by both state and nonstate actors and its potential disruptive capabilities for certain industries, firms that do not explore blockchain's impact risk obsolescence or increased regulation."[58] At this point, however, I recommend that corporate boards approach this technology cautiously, and it appears that they *are* proceeding with care. In a 2018 survey of Corporate Information Officers regarding blockchain adoption within their organizations, only 1% indicated any kind of organizational blockchain adoption; only 8% were planning or considering experimenting with blockchain; and 77% reported no interest in the technology and/or no action planned to investigate or develop it.[59] Corporations certainly are aware of and interested in blockchain's corporate governance, cybersecurity/data protection, and environmental, social and governance disclosure potential,

---

[57] Jeremy M. Sklaroff, Comment, *Smart Contracts and The Cost of Inflexibility*, 166 U. PA. L. REV. 263, 302 (2017).

[58] *See supra* note 1.

[59] *Hype Killer—Only 1% of Companies Are Using Blockchain*, Gartner Reports, Artificial Lawyer (May 4, 2018), https://www.artificiallawyer.com/2018/05/04/hype-killer-only-1-of-companies-are-using-blockchain-gartner-reports/.

but they may, like most governments, be waiting for the technology to mature as well as seeking to identify professionals to implement blockchain technology, including technologically-proficient lawyers.