Making Smart Contracts "Smarter" with Arbitration

Amy J. Schmitz describes the development of "smart contracts" and the challenges in resolving disputes in this arena. She explains the need for sound dispute system design complete with an arbitration provision built into smart contracts. She is an arbitrator with the American Arbitration Association, and the Elwood L. Thomas Missouri Endowed Professor at the University of Missouri School of Law.
https://law.missouri.edu/person/amy-j-schmitz/

The commercial world is increasingly reliant on technology, while the legal field has begrudgingly followed suit in order to remain relevant, and competent, in the wake of the digital revolution.[1] Business partners no longer rely on physical handshakes and inked documents. In fact, technology is revolutionizing the art of deal-making.[2] We now expect to make most purchases online through e-contracts, sealed with a click on the "accept" button.[3] Even corporate leaders now use e-mails and texts to negotiate deals, which they eventually "sign" online through services like Docusign.[4]

Despite our current comfort with these new types of online contracts, "smart contracts" on the blockchain push the envelope even further into the digital age. Smart contracts are different from common e-contracts in that they are essentially computer code.[5] Those with no coding background cannot easily interpret a smart contract in its rawest form.[6] Notably, smart contracts are not necessarily contracts and not necessarily "smart."

Instead, smart contracts are made up of "nodes" which consist of computer coded algorithms that live in a decentralized ledger.[7] A decentralized ledger, such as blockchain or ethereum, is a computer-coded ledger spread throughout computers instead of being centralized in one computer or database.[8] This decentralization helps make smart contracts nearly unhackable. Furthermore, these decentralized ledgers are immutable, meaning that the code generally cannot be altered. In other words, most distributed ledgers are "append only," meaning that parties may add to, but not alter, information placed in the ledger.

1.*See generally* RICHARD SUSSKIND, TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE (Oxford Univ. Press 2013).
2.AMY J. SCHMITZ & COLIN RULE, THE NEW HANDSHAKE: ONLINE DISPUTE RESOLUTION AND THE FUTURE OF CONSUMER PROTECTION, at ix (2017).
3.*Id.*
4.*Companies Using Verisign*, IDATALABS (2017), https://idatalabs.com/tech/products/verisign.
5.David Zaslowsky, *What to Expect When Litigating Smart Contract Disputes*, LAW360 (Apr. 4, 2018, 5:11 PM), https://www.law360.com/articles/1028009/what-to-expect-when-litigating-smart-contract-disputes.
6.*Id.*
7.Jakub J. Szczerbowski, *Place of Smart Contracts in Civil Law. A Few Comments on Form and Interpretation*, SSRN 333 (Jan. 8, 2018), https://ssrn.com/abstract=3095933.
8 For a simple explanation of smart contracts, *see* Adil Haris, *Smart Contracts—A Simple yet Comprehensive Explanation in Pictures*, at https://hackernoon.com/smart-contracts-a-simple-yet-comprehensive-explanation-in-pictures-bc21c7ab89b6.

This immutability and decentralization foster data safety. Accordingly, companies place data in the blockchain or another distributed ledger in order to manage risk. Furthermore, blockchain-based smart contracts create efficiencies and resolve transactional trust issues. The idea is that smart contracts may largely eliminate the need for complicated and costly letters of credit, bonds, and security agreements by digitizing automatic enforcement or payment in immutable computer code. At core, smart contracts codify if-then actions that may mimic contracts if built on a prior agreement, or could simply carry out payment or enforcement based on objectively delineated facts.[9] Examples of if-then actions are "If it rains, X gets an umbrella," or "If the goods reach port A, B gets paid."

The problem is that no amount of computer code can eliminate conflicts. An oracle, or third party fact verification system, could incorrectly detect rain, code may be flawed, there may be disputes about what qualifies as "rain" (mist, fog, sleet), etc. Furthermore, parties may fight about delivery of defective goods, leaving parties with no choice but to attempt litigation to recoup losses.[10] Aside from resetting – i.e, shutting down – the whole "if/then" system, these kinds of disputes present a challenge for immutable blockchain architectures.[11] Accordingly, parties are wise to plan ahead and build arbitration into their smart contracts, in order to have a dispute resolution plan should smart contracts go awry. This Article unpacks related issues and suggests a "plan."

The Role of the Blockchain in Smart Contracts

One of the key technologies behind smart contracts is the blockchain, or another digital ledger. This is essentially a distributed database, with data spread across the internet. It allows for information to be entered into the system and stored in different, redundant locations located throughout the world. When a document is put into the blockchain, it is replicated across every archival node, keeping data available even if half of the nodes, or computers, go down. Imagine if you had a notepad where everything you wrote in the notepad would be duplicated exactly in other notepads around the world, and each replication would include new information that is added. Even if you spilled coffee on one notepad, the information would still be preserved in the replications.

Also, imagine if there were safety "rules" around what information can be added to this notepad. If someone tried to write something in a notepad that didn't follow the rules, then all the other notepads would reject it. This is another feature of the blockchain: if someone provides an update that doesn't follow the network rules, then the other nodes will evaluate the contribution and determine the update doesn't comply, so they will not add it to the definitive ledger. That makes spoofing or editing information previously submitted into the blockchain extremely difficult, if not impossible. Indeed, it generally takes a "super computer" to even attempt the necessary computing challenges involved in "hacking" the blockchain.

---

[9] *See* Amy J. Schmitz & Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 JOURNAL OF DISPUTE RESOLUTION 103 (2019); Amy Schmitz, Blockchain, Smart Contracts, and ODR - from Cyberweek 2019, YouTube.
[10] Riikka Koulu & Kalle Markkanen, *Conflict Management for Regulation-Averse Blockchains?*, *in* REGULATING INDUSTRIAL INTERNET THROUGH IPR, DATA PROTECTION AND COMPETITION LAW 8-10 (R.M. Ballardini, O. Pitkänen, & P. Kuoppamäki eds., forthcoming).
[11] *Id*.

This makes smart contracts built into the blockchain incredibly powerful. As noted above, smart contracts are already self-enforcing computer programs, but they become more secure when programmers drop them into the blockchain. Smart contracts eliminate the need for paper documents, wet ink signatures, and—for the most part—courts and lawyers. Smart contracts lodged in the blockchain strive for auto-enforcement through code instead of judges and courts.[12]

Ideally, blockchain also provides safety because it provides encryption with public and private keys, which are blockchain-based identification numbers provided by the network.[13] In reality, however, blockchain is not impenetrable. It is more secure than general cloud-based systems, but it can be "hacked" and has its own risks.[14] Hackers could manipulate the technology by, for example, using a "hard fork" to essentially create a copy of the blockchain which might allow unscrupulous parties to manipulate the data and essentially "steal" information. Indeed, a well-executed "hard fork" could even make a blockchain vulnerable to corruption and collapse.[15]

At the same time, blockchain is evolving and moving far beyond its origins in cryptocurrencies like Bitcoin. The central objective of the blockchain was to create a self-regulating network that would enable the transfer of property between peers without the oversight of a third party, namely the courts and regulators.[16] However, the original Bitcoin system has been improved in newer platforms like Ethereum, and even private chains are thriving to allow for efficiencies and security in a range of industries.[17]

There has been a growth in initial coin offerings ("ICOs"), which are now recognized by the Securities and Exchange Commission and regulated as securities.[18] Furthermore, smart contracts have gained prevalence in banking, finance, insurance, and supply chain management, while law firms are building blockchain departments.[19] Their business clients have been experimenting with blockchain through venues like the Accord Project consortium. [20] Meanwhile, major tech companies like IBM and standard setting groups like the IEEE have been working to set common data and performance standards for smart contracts, which are crucial for wide acceptance.[21] In fact, ninety percent of Australian, European and North American banks are

12. Marco Dell'Erba, *Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation* 27-28 (Aug. 20, 2018), https://ssrn.com/abstract=3228445.
13. *Id.* at 9.
14. Angela Walch, *Blockchain's Treacherous Vocabulary: One More Challenge for Regulators*, 21 J. INTERNET L. 1, 5-7 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3019328.
15. *Id.* at 2-7. Instead of claiming the technology is "tamper-proof," some proponents now call it "tamper-resistant." *Id.*
16. *See generally* Walch, *supra* note 14.
17. Brant Carson et al., *Blockchain Beyond the Hype: What is the Strategic Business Value?*, MCKINSEY DIGITAL (June 2018), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.
18. *Id.*
19. Roger Aitken, *Accord Project's Consortium Launching First Legal 'Smart Contracts' with Hyperledger*, FORBES (July 26, 2017), https://www.forbes.com/sites/rogeraitken/2017/07/26/accord-projects-consortium-launching-first-legal-smart-contracts-with-hyperledger/#34781496472c.
20. *Id.*
21. *IBM Joins Accord Project Smart Contract Consortium*, ARTIFICIAL LAW (June 28, 2018), https://www.artificiallawyer.com/2018/06/28/ibm-joins-accord-project-smart-contract-consortium.

"experimenting" with using blockchain to verify and transfer financial "information and assets."[22] Additionally, twenty-five governments are piloting blockchain platforms.[23]

Nonetheless, blockchain and smart contracts are relatively nascent.[24] It will take some time for the industry to mature and develop, and it is unknown whether it will continue to expand or remain focused in niche areas. Furthermore, these unknowns, along with realities of technology in general, are sure to create conflicts. Disputes will develop and parties will seek means for resolving these disputes and obtaining remedies.

Trade "Wars" in the Blockchain

Pindar Wong, the chairman of VeriFi (Hong Kong) Ltd and co-founder of the first licensed internet service provider in Hong Kong in 1993, has argued that these robust smart contracts could diminish the impact of trade wars.[25] Mr. Wong observed:

> Trade warriors are fighting yesterday's battles. Instead of pitting their smokestack, 20th-century factories and armies of workers against each other, governments should apply blockchain's "Don't Trust, Verify" approach to trade arrangements, using it to reduce trade friction and improve cross-border relations to the betterment of their societies.[26]

The idea is that smart contracts allow parties to avoid tariffs and turf wars because they are housed in a decentralized ledger, and they guarantee performance or payment because the performance or payment is translated into immutable code. Moreover, this ledger is transparent, allowing parties to track shipments, payments, and other transactional occurrences every step of the way – without need for reliance on governments or even humans (assuming correct coding of the data). Furthermore, trust could be inherent with the transparency and automatic enforcement of the coded performance. Nonetheless, disputes will develop and a new kind of "trade war" could develop.

For starters, as noted above, there will be coding errors and disputes about the veracity and interpretation of the code. There is even a risk that fake data will improperly trigger, or fail to trigger, smart contract clauses. Computer coders could face damages for creating improperly structured contracts, while hackers may attempt to manipulate data to the advantage of one party or the other.[27] Parties may fight about whether the code accurately memorializes their agreement, and even coders may dispute "interpretation" of the code.[28] Indeed, there may be questions around the legality of smart contracts in some jurisdictions.

22.Carson et al., *supra* note 17.
23.*Id.*
24.*Id.*
[25] Pindar Wong, *Blockchain's Killer App? Making Trade Wars Obsolete*, COINDESK, May 21, 2018.
[26] *Id.*
27. *Id.*
28. Duncan Kennedy, *From the Will Theory to the Principle of Private Autonomy: Lon Fuller's "Consideration and Form,"* 100 COLUMBIA LAW REVIEW 94, 103 (2000); Lon L. Fuller, *Consideration and Form*, 41 COLUMBIA LAW REVIEW 799, 800-01 (1941).

At the same time, because each node of a blockchain ledger is potentially located in a different part of the world, blockchain ledgers do not have a clearly identified location or jurisdiction for each transaction. It is possible that parties could code jurisdictional choice into their smart contracts, but even that may be subject to public policy and statutory challenge within any one nation's courts. Even if parties choose jurisdictions with laws requiring enforcement of smart contracts, traditional courts may not have capacity and expertise to decide the disputes, and the inefficiencies of traditional courts would thwart the benefits of smart contracts.

In addition to questions around litigating smart contract disputes, questions loom regarding responsibility and accountability within the blockchain or other distributed ledger systems. By the nature of blockchain, there is no single owner of a blockchain system. That means that it is unclear who should be held accountable for any flaw or failure. The very ethos is libertarian in the sense that communal "law" and shared understandings should govern operations.

The immutability of blockchain also raises questions of data privacy, which may create yet more disputes around data. Cross-border blockchain platforms are examples of public networks that will handle personal data. It will be difficult to balance an individual's right to privacy in an open network, especially considering that many blockchain networks have little control over where data will be transferred and who has access to that data. Considering that, by its nature, blockchain is both transparent and private, should or does it matter who has access to the data? This creates especially thorny issues in light of the GDPR and other data legislation in various jurisdictions.

In sum, expected and unforeseen disputes will arise regarding smart contract coding and execution. Accordingly, parties are wise to build a dispute resolution plan into their blockchain strategy. Some disputes are inevitable as is true with any form of contract (smart or otherwise). Coding for possible breaches of contract can go only so far because there will always be a lack of foresight and information, as well as unpredictable human behavior.[29] At the same time, traditional litigation fails to address smart contracts' need for remedies that preserve anonymity and fit within the blockchain culture. Courts and traditional processes simply will not work for resolving many smart contract disputes.

The Need for Arbitration Built into the Blockchain

Currently, the leading means for regulating smart contracts seems to be to "reset" the system to avoid further damage. But this does not provide actual decisions on the disputes or remedies for those harmed. In other words, this is a measure to "stop bleeding" and does not resolve the disputes.

That said, there is some movement toward crowdsourced online dispute resolution (ODR). ODR providers like Kleros allow for this crowdsourced ODR by having token holders essentially be the jury and look at the evidence presented by each side. These token

29. Schmitz & Rule, *supra* note 9, at 110-115.

holders/jurors, who can be anyone who purchases tokens, then vote with tokens on the party that they think should "win" a given dispute. These token holders do not need any special background and remain anonymous, but they are "peers" in that they understand and work with digital ledgers, at least enough to be token holders. The side with the most tokens wins, and the token holders who chose that winning side get to take back their tokens along with the tokens of the voters who choose the "losing" side. The idea relies on a game theoretic model; Kleros implements other measures to stop "cheating" and attempting to game the system. The question, however, is whether this crowdsourced ODR is the product of good system design. It is also debatable whether the "winning" side is necessarily the "just" or "correct" resolution.

Dispute system design goes beyond consideration of positive law to consider goals, stakeholders, context and culture, processes and structures, resources, and more involved in a given situation. This allows us to think about the dispute resolution system in a much more contextualized way, responsive to the unique needs and expectations of a particular socio-legal culture. Parties to smart contracts are generally striving to protect privacy around their transactions and promote efficiency in business practices, as these are important goals behind smart contracts. Furthermore, access to decisionmakers with technological expertise would be vital for smart contract disputes. Indeed, one of the greatest fears around smart contract litigation is that generalist judges and juries lack necessary understanding of the complex technological issues often looming behind smart contract issues.

Accordingly, parties would be wise to address smart contract dispute resolution and establish best means for resolving these disputes in their smart contracts. Legislators passing laws stating smart contracts are enforceable generally do not understand what smart contracts are, let alone the best means for resolving related disputes. Even tokenized ODR is more in tune with dispute system design than the default – "reset" the system and simply stop the bleeding once a smart contract goes awry. But tokenized ODR may be vulnerable to risks if not properly devised.

Instead, users of smart contracts may want to build arbitration into their code to promote efficiency, protect privacy and ensure an expert decisionmaker. Furthermore, users may want to specify allowance for online arbitration to augment this efficiency, especially given the cross-border nature of most smart contracts. Smart contract dispute resolution should honor and support the efficiency of smart contracts. Furthermore, smart contract users may want to even further support these dispute resolution mechanisms by placing disputed funds in escrow while arbitration takes place to help ensure trust and enforcement of decisions.

Ideally, a well-designed online arbitration system for smart contract disputes would provide resolutions outside of the legal and political confines of the courts. Online arbitration built into the blockchain would provide resolutions outside the gaze of any one national policy or court. For further discussion, see Amy J. Schmitz and Colin Rule, *Online Dispute Resolution for Smart Contracts*, 2019 JOURNAL OF DISPUTE RESOLUTION 103 – 125 (2019).