

NEW YORK UNIVERSITY
JOURNAL OF INTELLECTUAL PROPERTY
AND ENTERTAINMENT LAW

VOLUME 9

FALL 2019

NUMBER 1

TOWARDS ENHANCED OVERSIGHT OF “SELF-
GOVERNING” DECENTRALIZED AUTONOMOUS
ORGANIZATIONS: CASE STUDY OF THE DAO AND ITS
SHORTCOMINGS

KYUNG TAECK MINN*

INTRODUCTION.....	140
I. THE HISTORY OF DISTRIBUTED LEDGER TECHNOLOGY, BLOCKCHAINS, AND SMART CONTRACTS	142
II. THE DAO AND ITS DOWNFALL.....	149
A. <i>The Mechanics and History of the DAO</i>	149
B. <i>The SEC Investigation of the DAO</i>	152
1. <i>The Curators Designated by Slock.it Had Unfettered Power Within The DAO</i>	152
2. <i>The Voting Rights of The DAO Investors Did Not Afford Them Meaningful Control Over the Enterprise</i>	154
III. THE MYTH OF SELF-GOVERNANCE OF TRADITIONAL CONTRACTS AND CORPORATIONS.....	156
A. <i>The Theory of Incomplete Contracts</i>	156
B. <i>The Failure of “Self-Enforcing” Corporate Law in Post-Soviet Russia</i>	158
IV. THE NEED FOR DISPUTE RESOLUTION BY NEUTRAL THIRD-PARTIES IN DAOs	160

* J.D. candidate, 2020 New York University School of Law.

A. <i>What to Enforce: Fiduciary Duties from Corporate Law and The Doctrine of Public Policy from Contract Law</i>	162
1. <i>The Fiduciary Duties of Loyalty and Due Care</i>	162
i. <i>The Duty of Loyalty</i>	163
ii. <i>The Duty of Due Care</i>	164
2. <i>The Doctrine of Public Policy</i>	165
B. <i>Which Neutral Third-Party Will Adjudicate: Courts, Arbitrators, or Blockchain Dispute Resolution Services</i>	167
1. <i>The Court System</i>	168
2. <i>Arbitration</i>	170
3. <i>Blockchain Dispute Resolution Services</i>	171
4. <i>The Unique Problem of Enforcement</i>	132
C. <i>Who Will Enforce: Private Investors or Government Regulatory Agencies</i>	174
1. <i>Private Investors</i>	174
2. <i>Government Regulatory Agencies</i>	176
CONCLUSION.....	177

INTRODUCTION

Blockchain, cryptocurrency, smart contracts—these obscure terms began flooding the news a few years ago and for good reason. These are technologies with the potential to fundamentally change the way in which society performs its business transactions.

The blockchain, in layman’s terms, is a “ledger [that] is kept and updated communally by all the computers that are hooked into the [blockchain] network.”¹ Because the ledger is kept communally, no single computer or institution is in charge of the financial data on the ledger.² “If any one computer keeping the records is hacked or knocked offline, the other computers can go on without it.”³ Because of this property, blockchain technology is of particular interest to companies that manage large amounts of data. It represents an opportunity to make databases resilient to tampering.⁴ Apart from the security benefits, blockchains can potentially

¹ Nathaniel Popper, *What Is the Blockchain? Explaining the Tech Behind Cryptocurrencies*, N.Y. TIMES (June 27, 2018), <https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-information.html>.

² *See id.*

³ *Id.*

⁴ *See id.*

provide a solution to keeping multiple copies of a database synchronized.⁵ That is why Fortune 500 companies are investing billions of dollars into blockchain technology.⁶ Samsung Electronics, AXA Group, and Bank of America are just a few of the myriad companies that are developing blockchain technologies for a variety of applications such as tracking global supply chains, automatically executing insurance payments, and creating letters of credit.⁷

Large corporations aren't the only ones that can benefit from blockchain technology. Average consumers can use smart contracts, programmable automated transactions that operate and store their records on the blockchain, as a secure way to buy goods and services from online markets.⁸ Smart contracts can even be programmed as an investment vehicle, similar to a mutual fund, to receive capital from multiple investors and invest them in another enterprise. Unlike mutual funds, these smart contracts lack an ostensible fund manager. Decisions on how to manage the fund are made via a majority vote amongst the investors. Such smart contracts are called "Decentralized Autonomous Organizations" or "DAOs." In fact, investors have already shown explosive interest in such ventures. The first smart contract of such a kind, The DAO, raised \$150 million over the course of four weeks in mid-2016, making it the most successful crowdfunded project in history at the time.⁹

Despite the eagerness of investors to dive into DAOs, DAO smart contracts, like any other contract, are imperfect and unable to completely escape the risk of governance problems and contractual disputes. DAO smart contracts are programmed to have their parties resolve such disputes through "self-governance." That is, parties to a DAO will resolve disputes through majority vote, without relying on a central legal authority. However, unguided and unchecked dispute resolution in

⁵ *See id.*

⁶ *See* Andrew Ross Sorkin, *Demystifying the Blockchain*, N.Y. TIMES (June 27, 2018), <https://www.nytimes.com/2018/06/27/business/dealbook/blockchain-technology.html>.

⁷ *See* Michael del Castillo, *Big Blockchain: The 50 Largest Public Companies Exploring Blockchain*, FORBES (July 3, 2013), <https://www.forbes.com/sites/michaeldelcastillo/2018/07/03/big-blockchain-the-50-largest-public-companies-exploring-blockchain/#33bc337d2b5b>.

⁸ *See* Nathaniel Popper, *Ethereum, a Virtual Currency, Enables Transactions that Rival Bitcoin's*, N.Y. TIMES (Mar. 27, 2016), <https://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html>.

⁹ *See* Nathaniel Popper, *A Venture Fund with Plenty of Virtual Capital, but No Capitalist*, N.Y. TIMES (May 21, 2016), <https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html>.

such a nascent area of technology, still mostly beyond the reach of the law, will most certainly result in unfair outcomes and processes.

This Note proposes that fair, self-governed resolution of governance problems and disputes within a DAO is unrealistic. Further, this Note calls for the intervention of neutral third-parties in the blockchain ecosystem to adjudicate disputes fairly, enforce fiduciary duties, and promote public policy. This Note also proposes that among the variety of tribunals that could adjudicate such disputes, traditional courts are most appropriate for the role. Finally, this Note proposes that government regulatory agencies are best suited to prosecute such cases.

Part I of this Note presents an overview of distributed ledger technology, blockchains, smart contracts, and DAOs. This part provides a deep dive into the motivation behind the development of each technology. Part II is a case study of The DAO. Although The DAO did not last long enough for serious governance problems to emerge, an analysis of The DAO’s voting system reveals a highly problematic governance system. Part III examines traditional economics literature and extracts lessons supporting this Note’s thesis that self-governance of DAOs is futile. Part IV proposes a set of substantive rules that should be imposed on DAOs and also highlights the neutral third-parties that can adjudicate disputes arising from violations of those substantive rules. The final section concludes this Note.

I

THE HISTORY OF DISTRIBUTED LEDGER TECHNOLOGY, BLOCKCHAINS, AND SMART CONTRACTS

Computing technology has pervaded all aspects of the legal practice, and financial contracts represent a significant area of interest. Transferring a natural-language financial contract into a format that can be processed electronically presents opportunities for the automatic execution and enforcement of contracts without the need for courts, and consequently, the reduction of transaction costs. One such example is a “smart contract.” The idea of digitizing and automating contracts was popularized in 1994 when Nick Szabo coined the term “smart contract” to describe “a computerized transaction protocol [, or a computer program,] that executes the terms of a contract.”¹⁰ Szabo envisioned that smart contracts would “satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious

¹⁰ NICK SZABO, SMART CONTRACTS (1994), <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.

and accidental, and minimize the need for trusted intermediaries.”¹¹ Szabo intended smart contracts to minimize fraud and reduce transaction costs including arbitration and enforcement costs.¹²

A smart contract can be analogized to a vending machine. As long as the machine has inventory and money is properly inserted into the machine, a contract for the sale of a bottled beverage will be automatically executed. Smart contracts can also govern more complicated financial transactions that may require inputs from the parties over the course of its execution. In a car insurance smart contract for example, the driver can enter an input detailing a car accident. Such inputs can trigger predetermined steps according to the terms of the car insurance smart contract—the determination of whether the driver previously defaulted on monthly premiums, the delivery of an insurance payout, and the adjustments to the insurance rate—which can then be automatically executed by a computer.

The models and technologies for automatically executing contractual provisions (e.g., the transfer of assets upon satisfaction of pre-defined conditions) have experienced continuous innovation with some implementable forms emerging in the early 2000s. Yet, smart contracts did not see widespread utilization until only recently. The main problem preventing implementation was both parties to a transaction each having to have two separate instances of a smart contract program run on two separate systems (unless a party concedes to running only one instance of the smart contract on their counterparty’s system as in the car insurance smart contract example *supra*). Realizing a functional smart contract would be further complicated if the parties disagreed on the smart contract code and decided to program their own versions of the smart contract; the parties would then run the risk of the two versions producing different results in practice. However, the development of the distributed ledger in 2008 brought a platform on which a common smart contract could be hosted and executed.

A distributed ledger “is a digital record that is shared instantaneously across a network of participants.”¹³ It functions by storing identical copies of the digital record with each of the individual users (or nodes) on the network. In the smart contract context, whenever a new transaction occurs and the ledger must be updated, each copy of the ledger is simultaneously updated with new information. However, the update is only made possible when the majority of nodes agree on the new

¹¹ *Id.*

¹² *See id.*

¹³ INT’L SWAPS AND DERIVATIVES ASS’N & LINKLATERS, WHITEPAPER: SMART CONTRACTS AND DISTRIBUTED LEDGER - A LEGAL PERSPECTIVE 7 (2017).

changes by each individually verifying the new transaction against the preexisting ledger. This ensures that there is no deviation within the multiple copies of the data and only a single version of the record exists, albeit stored on multiple nodes. That single record represents a golden source of data that cannot be tampered with. A malicious hacker could alter the transactions kept on a centralized ledger with relative ease, but simultaneously infiltrating a majority of nodes in a large distributed ledger network would be a near impossible task.

The blockchain is the quintessential implementation of distributed ledger technology. Think of the blockchain as a database, maintained by all the nodes on the blockchain network, that is structured as a chronologically ordered, linear series of data “blocks.” Each block serves as a record of transactions with the latest block on the blockchain aggregating the most recent transactions.¹⁴ Before being added to the blockchain, the latest block must be broadcasted to and verified by a majority of the nodes on the entire blockchain network. Once the nodes reach consensus, the latest block is appended to the block that immediately precedes it in the blockchain by an encrypted reference.¹⁵ This results in the entire transaction history of the network being recorded in a series of data blocks connected through chains of encrypted references, hence the name “blockchain.” Once a new block is added, updated copies of the blockchain record are distributed to each individual user for future verification purposes. The append-only nature of the blockchain makes transactions on the blockchain irreversible. Today, the term “blockchain technology,” technically a subset of its mother technology, has become synonymous with distributed ledger technology and this Note uses the two terms interchangeably. Some of the largest functioning blockchains today include the Bitcoin and Ethereum blockchains.

¹⁴ See Bitcoin Wiki, *Block*, <https://en.bitcoin.it/wiki/Block> (as of Dec. 5, 2018).

¹⁵ See *id.*

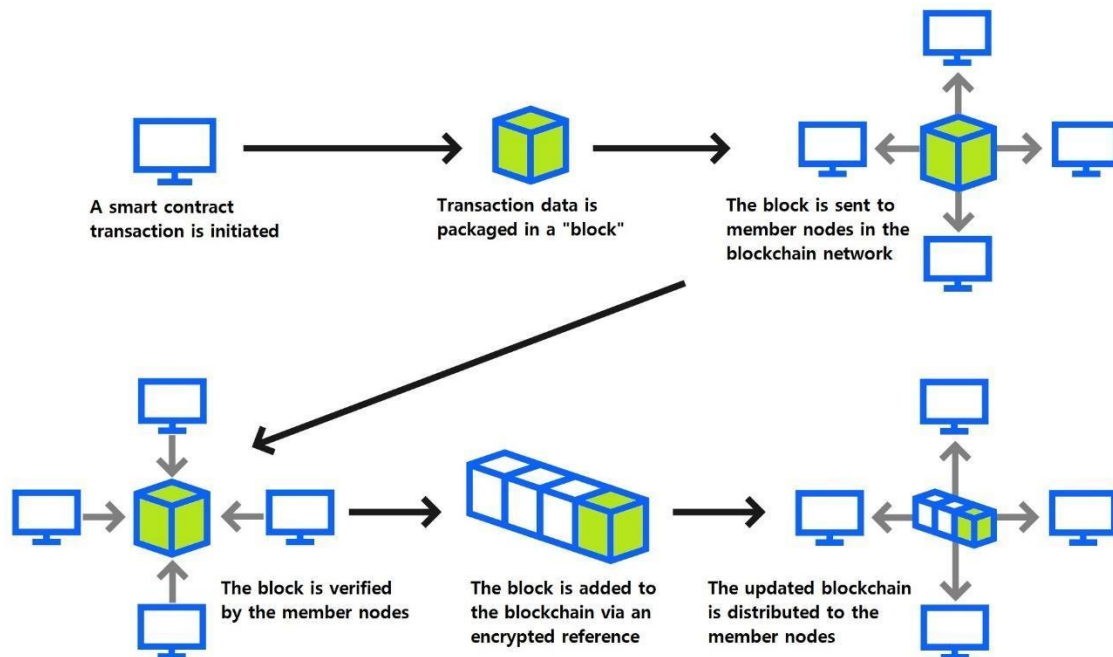


Figure 1. How a smart contract transaction is incorporated into a blockchain

Blockchains employ virtual currencies to act as mediums of exchange for their transactions. These currencies, dubbed “cryptocurrencies,” are programmed specifically to function on decentralized networks that lack any kind of central authority. Werbach and Cornell’s explanation on cryptocurrencies sheds light on the subject:

The core attribute of [cryptocurrency] is that it allows unrelated individuals and organizations to have confidence in transactions without trusting intermediaries or a legal system. A currency requires trust because buyers and sellers must believe that the tokens they exchange for assets of value will themselves have value. A one hundred dollar bill without the “full faith and credit” of the United States of America is just a piece of paper featuring a green portrait of Benjamin Franklin. [A cryptocurrency] supplies a mechanism of trust that does not require the backing of any trusted institution or government. And that same mechanism can be employed for other kinds of transactions.¹⁶

¹⁶ Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 325 (2017) (citation omitted).

The aforementioned mechanism of trust is supplied when cryptocurrencies are secured by “cryptography rather than traditional means.”¹⁷

What does it mean for a virtual currency to be secured by cryptography? On the blockchain, parties can set up an “account,” comprised of a public address (a “public key”) and a password (a “private key”).¹⁸ To transfer funds in the course of a transaction, a user of the blockchain finds another user’s public key, transfers cryptocurrencies, and inputs their private key, sealing the transaction with a “digital signature.”¹⁹ This process ensures that all transactions are authenticated and non-repudiable. The party that authorized the transfer of funds in a disputed transaction will have a difficult time arguing that they did not engage in a transaction unless they can prove that their private key was compromised.²⁰

The usage of blockchain and cryptocurrencies for transactions uniquely enables smart contracts. Storing the transactional data and running the code of a smart contract on a blockchain network would guarantee that “there is only one ‘golden’ version [of the code and transaction history], which effectively binds both parties.”²¹ Furthermore, once the smart contract begins to run, both parties can take comfort in that the transaction will self-execute with neither party able to tamper with it.²² The transactions would be irreversible. Once a transferor securely sends cryptocurrencies to a transferee’s public address, it is impossible to transfer them back out without the transferee’s private key. The smart contract, in addition to its self-executing and irreversible properties, is also self-enforcing because withholding payment when the relevant condition is satisfied is not possible if the smart contract code does not allow for it.²³ Thus, when combined with blockchain technology and cryptocurrencies, the smart contract offers a self-executing, immutable, and self-enforcing alternative to the traditional methods of performing financial transactions.

Smart contracts on a blockchain are not limited to transactions between two parties; they can also govern transactions between multiple investors. Imagine a mutual fund—a smart contract can pool cryptocurrencies from investors and invest them in other ventures. But also imagine that mutual fund having voting rights

¹⁷ *Id.* at 315 n.3.

¹⁸ See Cardozo Blockchain Project, Cardozo School of Law, “*Smart Contracts*” & *Legal Enforceability*, Research Report No. 2 (Oct. 16, 2018) (https://cardozo.yu.edu/sites/default/files/2020-01/smart_contracts_report_2_0.pdf).

¹⁹ *See id.*

²⁰ *See id.*

²¹ INT’L SWAPS AND DERIVATIVES ASS’N & LINKLATERS, *supra* note 13, at 9.

²² *See id.*

²³ *See id.*

similar to a corporation—a smart contract can give its investors voting rights which can be used to influence how the cryptocurrencies are managed. It is possible for such a smart contract to also have an administrator responsible for coding the smart contract. Exactly how such a smart contract operates and manages its cryptocurrencies would depend on how the smart contract is coded and designed.

The smart contract discussed above can be seen as forming a for-profit organization encompassing numerous investors and potentially a code-developing administrator. The blockchain community has labeled such organizations, investors bound together by a smart contract, Decentralized Autonomous Organizations or DAOs.²⁴ Despite having some characteristics of a corporation, such as shareholders and voting rights, it is ambiguous whether a DAO can be classified as a corporation since it has not been formed under the corporate laws of any jurisdiction. As a result, it is unclear what body of law should apply to such an organization, and they are not currently recognized as legal entities.²⁵

One of the primary aims behind the design of DAOs is to tackle the principal-agent problem.²⁶ Such a problem “arises whenever the welfare of one party, termed the ‘principal’, depends upon actions taken by another party, termed the ‘agent’ [A]most any contractual relationship, in which one party (the ‘agent’) promises performance to another (the ‘principal’), is potentially subject to an agency problem.”²⁷ Traditional corporations and investment funds are also subject to the principal-agent problem. One generic problem facing corporations and investment firms is the conflict between the firm or asset’s owners and its hired managers.²⁸ “The problem lies in assuring that the managers are responsive to the owners’

²⁴ See ALLEN & OVERY LLP, DECENTRALIZED AUTONOMOUS ORGANIZATIONS (July 2016), <http://www.allenoverly.com/publications/en-gb/Pages/Decentralized-Autonomous-Organizations.aspx>; Shermin Voshmgir, *Tokenized Networks: What is a DAO?*, BLOCKCHAINHUB (July 2019), <https://blockchainhub.net/dao-decentralized-autonomous-organization>. A DAO is not limited to being used as an investment vehicle, but this Note will limit its discussion to DAOs used for investment purposes.

²⁵ See Popper, *supra* note 9; ALLEN & OVERY LLP, *supra* note 24, at 5; CHRISTOPH JENTZSCH, DECENTRALIZED AUTONOMOUS ORGANIZATION TO AUTOMATE GOVERNANCE 1 (2016), <https://ia800603.us.archive.org/11/items/DecentralizedAutonomousOrganizations/WhitePaper.pdf>.

²⁶ See JENTZSCH, *supra* note 25, at 1

²⁷ John Armour, Henry Hansmann & Reinier Kraakman, *Agency Problems, Legal Strategies, and Enforcement* 2 (Harvard John M. Olin Center for Law, Economics, and Business, Discussion Paper No. 644 7/2009, 2009), http://www.law.harvard.edu/programs/olin_center/papers/pdf/Kraakman_644.pdf.

²⁸ See *id.*

interests rather than pursuing their own personal interests.”²⁹ To address this problem, rules describing permitted and proscribed conduct are imposed on managers by private contracts (e.g., corporate bylaws) and corporate law.³⁰ But whatever the rules may require, “[t]he core of the difficulty is that, because the [manager] commonly has better information than does the principal about the relevant facts, the principal cannot easily assure himself that the [manager’s] performance is precisely what was promised.”³¹ Consequently, “the [manager] has an incentive to act opportunistically, skimping on the quality of his performance, or even diverting to himself some of what was promised to the principal.”³² To assure that the manager does not shirk his responsibilities, the principal must engage in costly monitoring of the manager, which further reduces the value of the venture.³³ “While bad behavior may make a corporation or its management civilly or criminally liable, punishment can come as little comfort to an investor who has already lost their money.”³⁴ And not all investors will have the resources to bring an enforcement action in the first place.

Aware of the principal-agent problem, the architects of an early version of a DAO smart contract sought to circumvent the problem by eliminating, or, at least, diminishing the powers of, the problem’s cause, the manager. Created by Slock.it, a German corporation, and implemented on the Ethereum blockchain, “The DAO” operated according to a majority vote by its investors instead of entrusting the entirety of the investors’ assets to a central manager who decides how to manage the assets.³⁵ In addition, by having “governance rules [that were] automated and enforced using software,” The DAO did not even allow the choice of disobeying the governance rules that were hard-coded into the smart contract.³⁶

Despite its advantages and lofty ideals, The DAO still could not fully resolve its problems of governance and dispute resolution. Smart contracts are only as perfect as the humans that write their code, and The DAO was no exception. Bugs in smart contract software are as inevitable as misunderstandings or misrepresentations in traditional contracts. The DAO, through majority vote, resolved a crippling contractual dispute that led to its downfall. However, a deeper

²⁹ *Id.*

³⁰ See JENTZSCH, *supra* note 25, at 1.

³¹ Armour, *supra* note 27, at 2.

³² *Id.* (footnote omitted).

³³ *Id.*

³⁴ JENTZSCH, *supra* note 25, at 1.

³⁵ See *id.* at 2.

³⁶ *Id.* at 1.

look into The DAO incident reveals that, without judicial oversight, self-directed dispute resolution has the potential to lead to the suppression of minority “shareholders” in the smart contract, engender self-dealing, and allow for fraud.

II THE DAO AND ITS DOWNFALL

Central to the story of The DAO is Ether, one of the two leading cryptocurrencies used in the blockchain ecosystem today. Ether is the cryptocurrency used on the Ethereum blockchain and is the second most popular cryptocurrency behind Bitcoin. Ether can be exchanged for traditional fiat currency on online exchanges such as Coinbase.³⁷ The price of Ether has fluctuated between \$102 and \$335 in 2019.³⁸ At the time this Note was written on September 14, 2019, 1 unit of Ether was traded for \$190 on Coinbase.³⁹

Ether and the Ethereum blockchain have been continuously developed since 2013 by the Russian-Canadian programmer Vitalik Buterin. While the Bitcoin blockchain can also support smart contracts, the Ethereum blockchain has been widely regarded as the better platform for programming and publishing smart contracts. This is because “[E]thereum replaces [B]itcoin’s more restrictive language . . . with a language that allows developers to write their own programs. . . . The [Ethereum] language . . . supports a broader set of computational instructions.”⁴⁰ The focus of the Ethereum blockchain is to integrate real-world transactions into the blockchain ecosystem through the development of smart contracts.

A. The Mechanics and History of The DAO

The DAO is perhaps the most infamous case of a self-governed resolution of a smart contract dispute. The DAO was one of the first implementations of a virtual organization existing on a blockchain seeking to use smart contracts to formalize, automate, and enforce governance rules similar to those in traditional corporations.⁴¹ Created by Slock.it, a German software company, and implemented on the Ethereum blockchain, The DAO was designed as a for-profit entity, similar to a mutual fund.

³⁷ See *How to Buy Ethereum*, COINBASE, <https://www.coinbase.com/buy-ethereum> (last visited Sept. 14, 2019).

³⁸ See *Ethereum Price Chart (ETH)*, COINBASE, <https://www.coinbase.com/price/ethereum> (last visited Sept. 14, 2019).

³⁹ See *id.*

⁴⁰ Alyssa Hertig, *How Do Ethereum Smart Contracts Work?*, COINDESK, <https://www.coindesk.com/information/ethereum-smart-contracts-work>.

⁴¹ See JENTZSCH, *supra* note 25, at 1.

The DAO would operate in a “decentralized” manner in that it would make decisions based on votes by investors.⁴² The DAO was to be “autonomous,” and would have a project proposal and voting process that would be automatically executed by the code of The DAO smart contract.⁴³

The lifecycle of The DAO began in 2016 by amassing Ether from investors. In exchange for the investors’ Ether, The DAO distributed DAO Tokens which were analogous to stock in a corporation; DAO Tokens represent both units of voting power and rights to The DAO’s profits.⁴⁴ After an offering period of approximately four weeks, The DAO solicited “proposals” for how its funds might be used.^{45,46} Any DAO Token Holder could submit a proposal on how to use The DAO’s Ether.⁴⁷ One example of the proposals submitted to The DAO is Slock.it’s own: a project “to design and manufacture a ‘smart’ lock system that would enable ‘sharing economy’ members (such as AirBnB homeowners) to programmatically grant access to their homes to approved renters.”⁴⁸ Investors would earn rent on each transaction that used the smart lock system and voted by allocating their DAO Tokens for specific proposals (since DAO Tokens could be converted into Ether, this was conceptually similar to crowdfunding a project).⁴⁹ Proposals had to be approved by a “Curator” before investors could vote on them.⁵⁰ Initially chosen by Slock.it, curators were individuals who screened proposals to determine whether they originated from an identifiable party⁵¹ and whether they had any fraudulent intent.⁵² After a screening process, curators would present the proposals to investors by adding them to a

⁴² See SEC. & EXCH. COMM’N, RELEASE NO. 81207, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 4 (2017) [hereinafter SEC. & EXCH. COMM’N].

⁴³ See *id.*

⁴⁴ See *id.*

⁴⁵ See Quinn DuPont, *Experiments in Algorithmic Governance: A History and Ethnography of “The DAO,” a Failed Decentralized Autonomous Organization*, in BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE 157, 160 (Malcolm Campbell-Verduyn ed., 2017).

⁴⁶ See JENTZSCH, *supra* note 25, at 2.

⁴⁷ See *id.*

⁴⁸ DuPont, *supra* note 45, at 161.

⁴⁹ See *id.* at 160.

⁵⁰ See SEC. & EXCH. COMM’N, *supra* note 42, at 7.

⁵¹ See *id.*

⁵² See JENTZSCH, *supra* note 25, at 2 (“For example, an attacker with 51% of the tokens, acquired either during the fueling period or created afterwards, could make a proposal to send all the funds to themselves. Since they would hold the majority of the tokens, they would always be able to pass their proposals.”).

“whitelist.”⁵³ The investors’ voting rights weren’t limited to voting on business proposals. Investors could propose and vote on a wide array of issues within The DAO, such as the election of a new curator and splitting The DAO into two.⁵⁴ Investors could even vote for specific decisions within approved projects such as the hiring of a new employee.⁵⁵ “The level of management granularity would be set by the [smart] contract . . . that runs on the blockchain, and projects could choose to have the minutia of decisions voted on by members, or decide to have only major decisions go to vote.”⁵⁶

After its launch on April 30, 2016, The DAO enjoyed widespread popularity within the blockchain community as it raised \$150 million-worth of Ether.⁵⁷ However, this success was short lived. In late May, “concerns about the safety and security of The DAO’s funds began to surface due to vulnerabilities in The DAO’s code.”⁵⁸ Finally on June 17, 2016, the codified implementation of The DAO smart contract diverged from its original intention. Several errors in the smart contract code written by the Slock.it team allowed a single “attacker” to drain approximately \$50 million-worth of Ether from The DAO.⁵⁹ The DAO smart contract code had a built-in security measure preventing the attacker from immediately exchanging the siphoned Ether off of the Ethereum blockchain and into traditional currency, but the fate of the stolen funds and that of The DAO were in limbo. The stolen funds could not be retrieved, even by the Slock.it programmers who wrote and administered the smart contract, because the only point of access would be through the attacker’s private key.

To secure the diverted Ether, Slock.it’s founders, the Ethereum Foundation, and The DAO’s biggest investors, with all their political clout in the blockchain community, pushed for a “Hard Fork” to the Ethereum blockchain.⁶⁰ A Hard Fork is an update to the blockchain’s protocol which would result in a completely new blockchain.⁶¹ Proponents of the Hard Fork, which included the Slock.it team, planned to revert the new blockchain to one that resembled the Ethereum blockchain

⁵³ See SEC. & EXCH. COMM’N, *supra* note 42, at 8.

⁵⁴ See JENTZSCH, *supra* note 25, at 2-3.

⁵⁵ See DuPont, *supra* note 45, at 160.

⁵⁶ *Id.*

⁵⁷ See SEC. & EXCH. COMM’N, *supra* note 42, at 2-3.

⁵⁸ See *id.* at 9.

⁵⁹ See *id.*

⁶⁰ See *id.*; see also DuPont, *supra* note 45, at 165.

⁶¹ See ALLEN & OVERY LLP, *supra* note 24, at 4.

before the launch of The DAO.⁶² This would also have the effect of returning all of the funds raised by The DAO, including those taken by the attacker, to The DAO investors.⁶³ In contrast to Slock.it’s stance on the issue, a minority of investors argued that “code is law” and that a Hard Fork would go against the very spirit of decentralized autonomous organizations.⁶⁴ These dissidents thought that “[t]he hard fork would amount to an intervention—a bail-out of The DAO—seemingly at the behest of The DAO’s biggest investors.”⁶⁵ The purpose of the Ethereum blockchain and The DAO, after all, was to provide an immutable transactional record and host smart contracts that would solve the principal-agent problem. Yet all those ideals seemed to take a back seat when the financial and reputational interests of blockchain authorities were on the line. This conflict between Slock.it and their dissenting investors was a quintessential smart contract dispute, with one party looking to respect the original intent of the smart contract and the other seeking to strictly uphold its language (or code). After a majority vote among all participants of The DAO, they executed the Hard Fork, and the new Ethereum blockchain went live on July 20, 2016.⁶⁶

B. The SEC Investigation of The DAO

On July 25, 2017, the Securities and Exchange Commission (“SEC”) issued a report on The DAO incident. Although the focus of the SEC investigation was to determine whether DAO Tokens were securities, the report still identified significant shortcomings in The DAO’s system of self-governance.

1. The Curators Designated by Slock.it Had Unfettered Power Within The DAO

The designers of The DAO smart contract created the curator position to protect investors from fraudulent proposals.⁶⁷ But, in doing so, The DAO inadvertently revived the managerial authority that it was meant to eliminate. The curators had “ultimate discretion as to whether or not to submit a [project] proposal for voting” by the investors.⁶⁸ The only guidelines that the curators had were to: (1) confirm that any project proposal for funding originated from an identifiable person or organization; and (2) confirm that the smart contracts associated with the project

⁶² See SEC. & EXCH. COMM’N, *supra* note 42, at 9.

⁶³ See ALLEN & OVERY LLP, *supra* note 24, at 4.

⁶⁴ See DuPont, *supra* note 45, at 165.

⁶⁵ ALLEN & OVERY LLP, *supra* note 24, at 4.

⁶⁶ See SEC. & EXCH. COMM’N, *supra* note 42, at 9.

⁶⁷ See JENTZSCH, *supra* note 25, at 2.

⁶⁸ SEC. & EXCH. COMM’N, *supra* note 42, at 8.

properly reflected its proposed intent.⁶⁹ If a curator determined that a proposal met these criteria, “[she] could add the proposal to the ‘whitelist,’ which was a list of Ethereum Blockchain addresses that could receive [funds] from The DAO if the majority of DAO Token holders voted for the proposal.”⁷⁰ Curators also held control over “the order and frequency of proposals, and could impose subjective criteria for whether the proposal should be whitelisted.”⁷¹ The curators themselves admit to wielding such immense power. One of the curators designated by Slock.it stated that “the curator had ‘complete control over the whitelist . . . the order in which things get whitelisted, the duration for which [proposals] get whitelisted, when things get unwhitelisted . . . [and] clear ability to control the order and frequency of proposals,’ noting that ‘curators have tremendous power.’”⁷² Another curator “publicly announced his subjective criteria for determining whether to whitelist a proposal, which included his personal ethics.”⁷³ The curators “also had the power to reduce the voting quorum requirement by 50% every other week” where the same effect would take place only if no proposal reached the minimum quorum requirement for 52 weeks.⁷⁴

It is evident that the curators, as the gatekeepers of \$150 million of digital funds, had great power and responsibility. However, Slock.it chose the curators unilaterally without soliciting any feedback from The DAO investors.⁷⁵ Instead of revealing any kind of selection process, Slock.it merely touted that the curators were well qualified and trustworthy.⁷⁶ The curators all appeared to live outside the United States and many of them were associated with the Ethereum Foundation, the developers of the Ethereum blockchain.⁷⁷ Slock.it, when programming The DAO’s smart contract code, contemplated no check on the curators’ power other than allowing investors to submit proposals for the replacement of a curator. It was the “curators [who] had the power to determine whether a proposal to remove curator was put to a vote.”⁷⁸

⁶⁹ *See id.* at 7.

⁷⁰ *Id.* at 8.

⁷¹ *Id.*

⁷² *Id.* (quoting Epicenter, *EB134—Emin Gün Sirer And Vlad Zamfir: On A Rocky DAO*, YOUTUBE (June 6, 2016), <https://www.youtube.com/watch?v=ON5GhIQdFU8>).

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *See id.* at 7.

⁷⁶ *See id.* n.25.

⁷⁷ *See id.*

⁷⁸ *Id.* at 13.

The DAO incident was too short-lived to have developed any problems warranting an enforcement action from the SEC, but the highly suspect power structure of The DAO was a recipe for serious governance problems. The DAO’s curators were the gatekeepers to proposals and thus have a strong say in how The DAO should use its funds. When considering that the curators had tremendous power, were difficult to remove, and had reason to endorse proposals favorable to Slock.it or the Ethereum Foundation, the notion that Slock.it had orchestrated a ripe opportunity to engage in self-dealing becomes quite plausible.

Imagine the following hypothetical: Slock.it submits a fraudulent proposal—disguised as legitimate—to the curators with the intent of funneling The DAO’s funds into its venture. The curators, who are supposed to act as a check against such sham proposals, list the venture on The DAO’s whitelist anyway because of their ties with Slock.it. At the voting stage, Slock.it, in league with The DAO’s biggest investors, manages to gather more than 51% of The DAO’s voting power and bulldozes the proposal through. Even if the minority investors figure out the scheme, any effort to protect their own funds, such as a proposal to split off their own funds into a new DAO, must go through the Slock.it-dominated curators and is unlikely to survive. The DAO’s system of self-governance left open the possibility of Slock.it and majority investors misappropriating the minority investors’ funds with no valid way for the minority investors to counteract Slock.it’s devices.

2. The Voting Rights of The DAO Investors Did Not Afford Them Meaningful Control Over the Enterprise

The voting rights of DAO Token holders were limited “because DAO Token holders’ ability to vote for contracts was a largely perfunctory one; and . . . DAO Token holders were widely dispersed and limited in their ability to communicate with one another.”⁷⁹ The DAO’s voting process was also designed to disincentivize voting against proposals.

First, DAO Token holders could only vote on proposals vetted by the curators. But that “clearance process did not include any mechanism to provide DAO Token holders with sufficient information to permit them to make informed voting decisions.”⁸⁰ With no formal report on the projects from the curators, investors were substantially reliant on any information fed to them by Slock.it management.

⁷⁹ *Id.* at 14.

⁸⁰ *Id.*

Second, the pseudonymity and dispersion of investors made it difficult for them to exchange information or join efforts to effect change within The DAO. “Investments in The DAO were made pseudonymously (such that the real-world identities of investors are not apparent), and there was great dispersion among those individuals and/or entities who were invested in The DAO and thousands of individuals and/or entities that traded DAO Tokens in . . . secondary market[s].”⁸¹ Slock.it did create and maintain online forums on which investors could discuss project proposals, but the forums were hopelessly inadequate to serve as a gathering place for investors to form voting blocs to assert actual control over The DAO.⁸² This was due to the Slock.it forums being open to pseudonymous non-investors as well as there being too many DAO token holders for them to effectively coordinate movements amongst themselves.⁸³ The inadequacy of the forums was “later demonstrated through the fact that DAO Token holders were unable to effectively address the Attack without the assistance of Slock.it.”⁸⁴ The pseudonymity and dispersion of investors diluted their control over The DAO.

Third, investors’ voting rights were further attenuated by The DAO’s biased voting process. “[A]s noted in a May 27, 2016 blog post by a group of computer security researchers, The DAO’s structure included a ‘strong positive bias to vote YES on proposals and to suppress NO votes as a side effect of the way in which it restricts users’ range of options following the casting of a vote.’”⁸⁵ The DAO’s smart contract would tie up the DAO Tokens used in a vote of a proposal until that proposal was resolved. DAO Token holders could avoid such restrictions by abstaining from voting; any DAO Tokens not used in a vote could be freely withdrawn or transferred.⁸⁶ “As a result, DAO Token holders were incentivized either to vote yes or to abstain from voting.”⁸⁷ Such a voting process would distort voting behavior, especially amongst smaller investors with fewer DAO Tokens to spare, and “would not accurately reflect the consensus of the majority of DAO Token holders.”⁸⁸

⁸¹ *Id.*

⁸² *Id.* at 15.

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.* at 7. (quoting Dino Mark et al., *A Call for a Temporary Moratorium on The DAO*, HACKING, DISTRIBUTED (May 27, 2016 1:35 PM), <http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/>).

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

The limited voting rights of The DAO investors further increased their susceptibility to self-dealing. A lack of meaningful information on the proposals, no effective way to share the little information that the investors did have, and a strong bias to abstain or vote affirmatively meant that investors were more likely to inadvertently vote for fraudulent, self-dealing proposals.

III

THE MYTH OF SELF-GOVERNANCE OF TRADITIONAL CONTRACTS AND CORPORATIONS

The problems revealed in the SEC investigation are not specific to The DAO nor are they unique to entities on the blockchain. Traditional economics literature suggests that successful self-governance of a contractual dispute or of a corporation is a myth.

A. *The Theory of Incomplete Contracts*

The theory of incomplete contracts anticipates situations where the resolution of contractual disputes without a neutral third-party would lead to inefficient and inequitable outcomes. Consider two risk-neutral parties, a seller and a buyer of chicken, that can each profit by engaging in a transaction. The two parties initially meet on date zero, the seller agrees to invest in a shipment of chicken on date one, and the exchange of the chicken is scheduled to occur on date two. If it were possible for the parties, at date zero, to enter a contract that covers the entire transaction period and accounts for all possible contingencies, the seller would have enough confidence to fully invest in the chicken at an early stage of the transaction, and both parties would benefit. However, because contracts are incomplete by nature (i.e., it is impossible to *ex ante* bargain over all aspects of the contract),⁸⁹ the risk of *ex post* contractual disputes is inevitable. Suppose the buyer and seller agree on a contract specifying the price, quantity, and grade of chicken. However, the contract is silent on the type of chicken (i.e., does not distinguish between stewing chickens and broiling chickens). The interpretation of such missing or ambiguous contractual terms is typically left to a court, which may look to sources such as custom or trade usage to fill in the gaps of the contract. Interpreting the contract without a neutral third-party, however, will leave the party with greater bargaining power free to demand deference to its own interpretation of the contract. A neutral third-party is necessary to fairly construe ambiguous clauses.

⁸⁹ See Sanford J. Grossman & Oliver D. Hart, *The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration*, 94 J. POL. ECON. 691, 699 (1986).

Even if the contract were free of ambiguities and clearly defined each party's obligations, its enforcement would be difficult without a neutral third-party. One kind of *ex post* dispute occurs on date one when the seller underinvests in the chicken out of fear of giving the buyer too much bargaining power on date two. This leads to an inefficient situation where the seller doesn't fully commit to a mutually beneficial transaction due to the seller's mistrust of the buyer, and the initial contract failed to account for that mistrust.⁹⁰ In such a dispute, the seller is apprehensive that the buyer will abuse his increased bargaining power at a later stage of the transaction when the seller has already invested heavily in the chicken. As a result, the seller refuses to invest in the full amount of chicken as specified in the contract made at date zero. Because the buyer's profitability is reliant on the seller fully performing his end of the bargain, the buyer has less bargaining power and may have to make some concessions if the two parties decide to renegotiate prior to date one.

Another kind of *ex post* dispute occurs when the seller does commit to an expensive investment in the chicken, but the buyer decides to abuse his bargaining position by opening renegotiations prior to the exchange of the chicken on date two. In this second kind of dispute, the seller has already sunk a great deal of capital into the chicken and is pressured to sell it off quickly. The seller is also likely to be incurring costs such as interest payments and storage fees that will continue to cut into his profit margins the longer the transaction is delayed. Knowing this, the buyer refuses to buy the full amount of chicken according to the terms decided on date zero. Because the seller's profitability depends on the buyer purchasing the entirety of the chicken without significant delay, the seller has less bargaining power and may have to yield to the buyer on some points if the two parties decide to renegotiate prior to date two.

Self-governance of such disputes is unlikely to be fair due to imbalances in bargaining power (favoring the seller on date one and the buyer on date two). In the absence of a neutral third-party, the party with greater bargaining power is likely to command more discretion with regards to the interpretation of the original contractual provisions and use it to produce an advantageous, but not necessarily accurate, reading of the contract. To control the exercise of discretion and prevent such inequitable and inefficient outcomes, a neutral third-party such as a court must intervene.

It is possible to draw parallels between hypothetical buyer-seller disputes and contractual disputes in the smart contract world. In a financial smart contract such

⁹⁰ See Patrick W. Schmitz, *The Hold-Up Problem and Incomplete Contracts: A Survey of Recent Topics in Contract Theory*, 53 BULL. ECON. RES. 1, 4-6 (2001).

as The DAO, when the smart contract deviates from its original intent due to bugs in the code or unforeseen circumstances, renegotiations are likely to favor the party holding the cryptocurrencies rather than the investors who gave up those assets. An entity like Slock.it would have the bargaining power in this situation—it has technical expertise in the smart contract code, insider information about the proposals, and most importantly, possession of the assets. This is especially true on the blockchain since an investor who has already fully committed to a smart contract venture by transferring his cryptocurrencies cannot freely withdraw his investment. Cryptocurrency assets that have been transferred to another blockchain user’s address, or wallet, can’t be taken back without the address-holder’s private key. Applying the theory of incomplete contracts to DAOs, it becomes clear that a neutral third-party is necessary to prevent potential abuses of superior bargaining power in smart contract disputes.

B. The Failure of “Self-Enforcing” Corporate Law in Post-Soviet Russia

Traditional economics literature also warns that the self-governance of corporations, resolving conflicts and policing conduct within a corporation without relying on courts, is also likely to fail. During the mass privatization of state-owned enterprises in the formerly centrally planned Russian economy, American law professors Bernard Black and Reinier Kraakman helped design “self-enforcing” corporate laws that would govern Russian joint stock companies.⁹¹ The scholars were cognizant that “the corporate laws of developed economies . . . depend upon highly evolved market, legal, and governmental institutions and cultural norms that often do not exist in emerging economies”⁹² and that Russia was infested with “insider-controlled companies, malfunctioning courts, weak and sometimes corrupt regulators, and poorly developed capital markets.”⁹³ Thus, Black and Kraakman sought to devise a set of laws that would vest substantial decision-making power in large outside shareholders with incentives to make beneficial decisions for a company.⁹⁴ Their model self-enforcing law would achieve enforcement “through actions by direct participants in the corporate enterprise (shareholders, directors, and managers), rather than indirect participants (judges, regulators, legal and accounting professionals, and the financial press).”⁹⁵ Black and Kraakman envisioned that such a law would minimize the need for formal enforcement by courts, incentivize

⁹¹ See Bernard Black & Reinier Kraakman, *A Self-Enforcing Model of Corporate Law*, 109 HARV. L. REV. 1911, 1912 (1996).

⁹² *Id.* at 1913.

⁹³ *Id.* at 1915.

⁹⁴ See *id.*

⁹⁵ *Id.* at 1916.

managers and controlling shareholders to obey the rules, and reduce self-dealing by corporate insiders.⁹⁶

Alas, the self-enforcing corporate law did not perform as expected, and privatization efforts in Russia were a massive failure.⁹⁷ Notwithstanding the law's effects, managers and controlling shareholders of major Russian companies engaged in extensive self-dealing which the government neglected to control.⁹⁸ In 1999, Black and Kraakman observed that "the Russian ruble has plunged; the Russian government has defaulted on both its dollar- and ruble-denominated debt, most banks are bankrupt; corruption is rampant, tax collection is abysmal, capital flight is pervasive, and new investment is scarce."⁹⁹ To say the least, the self-enforcing corporate law didn't work out too well.

The architects of the self-enforcing law identified several problems that contributed to the ineffectiveness of the self-enforcing corporate law, one of which is analogous to a problem faced by the blockchain world. "[M]ass privatization of large enterprises is likely to lead to massive insider self-dealing unless . . . a country has a good infrastructure for controlling self-dealing."¹⁰⁰ Black and Kraakman admit that "[t]he privatizers, ourselves included, underestimated the extent to which functioning law requires honest courts and prosecutors that can redress gross violations."¹⁰¹ Good laws take years to write and good institutions take years to build, but privatization in Russia happened much too rapidly for good laws and institutions to take root.¹⁰² Decent laws on securities, companies, and bankruptcy were adopted by 1998, but by that time corrupt company managers established their positions and opposed efforts to strengthen or enforce the laws.¹⁰³ The aftermath was a disaster: most company managers stole whatever assets their private enterprises had, killing otherwise viable companies.¹⁰⁴ Black and Kraakman observed that "Russia's core problem [in 2000 was] less lack of decent laws than lack of the infrastructure and political will to enforce them."¹⁰⁵ The self-enforcing corporate

⁹⁶ See *id.* at 1915-16.

⁹⁷ See Bernard Black et al., *Russian Privatization and Corporate Governance: What Went Wrong?*, 52 STAN. L. REV. 1731, 1733 (2000).

⁹⁸ See *id.*

⁹⁹ *Id.*

¹⁰⁰ *Id.* at 1734.

¹⁰¹ *Id.* at 1756.

¹⁰² See *id.* at 1753.

¹⁰³ See *id.*

¹⁰⁴ See *id.* at 1734.

¹⁰⁵ *Id.* at 1755.

laws, which the American scholars themselves created, already prohibited much of the rampant self-dealing by managers and large shareholders, but they were hopelessly ineffective when entrusted to apathetic courts and prosecutors.¹⁰⁶ Black and Kraakman concluded by warning that “a decent legal and enforcement infrastructure must precede or at least accompany privatization of large firms” to prevent widespread self-dealing.¹⁰⁷

Similar to Russia in the 1990s, there is no government or judicial oversight in the world of smart contracts to prevent insider self-dealing. In the United States, only Arizona and Tennessee have enacted legislation related to smart contracts, and even those bills merely acknowledge smart contracts as binding contracts.¹⁰⁸ Even regulatory bodies such as the SEC, despite retroactively ruling that The DAO should have registered the offer and sale of its DAO Tokens,¹⁰⁹ do not affirmatively seek to police the governance structures of similar entities on the blockchain. Lastly, there is no case law to provide guidance on smart contract disputes.¹¹⁰ Smart contracts are currently in a blind spot of the law and if Black and Kraakman teach us anything, it is that self-governance of corporation-like entities will fail in the absence of well-established legal institutions. If left to their own devices without legal intervention, a self-governing DAO will most likely engage in self-dealing at the expense of its investors.

IV

THE NEED FOR DISPUTE RESOLUTION BY NEUTRAL THIRD-PARTIES IN DAOS

Traditional economics literature predicts that The DAO’s self-governance would have broken down even if not for The DAO’s exploitation by the attacker. Future iterations of DAOs, even those that are equipped with superior code and are free of Slock.it’s curators, are unlikely to escape The DAO’s fate. This is because

¹⁰⁶ See *id.* at 1755-56 (“The reported price to stall a criminal investigation into, say, a business-related Mafia hit: \$50,000 in Moscow; less elsewhere.”).

¹⁰⁷ *Id.* at 1735.

¹⁰⁸ See Scott H. Kimpel & Chris Adcock, *The State of Smart Contract Legislation*, HUNTON ANDREWS KURTH LLP (Sept. 5, 2018), <https://www.blockchainlegalresource.com/2018/09/state-smart-contract-legislation/#page=1>; ARIZ. REV. STAT. ANN. § 44-7061 (2017); TENN. CODE ANN. § 47-10-202 (West 2018).

¹⁰⁹ See SEC. & EXCH. COMM’N, *supra* note 42, at 16.

¹¹⁰ See Scott A. McKinney et al., *Smart Contracts, Blockchain, and the Next Frontier of Transactional Law*, 13 WASH. J.L. TECH. & ARTS 313, 325 (2018).

there is “no such thing as a fully decentralized and autonomous organization”¹¹¹ as Voshmgir argues:

Depending on the governance rules, there are different levels of decentralization. While the network might be geographically decentralized, and have many independent but equal network actors, the governance rules written in the smart contract or blockchain protocol will always be a point of centralization and loss of direct autonomy. DAOs can be architecturally decentralized (independent actors run different nodes), and are geographically decentralized (subject to different jurisdictions), but they are logically centralized (the protocol). The question of how to upgrade the code—when and if necessary—is very often delegated to a set of experts who understand the techno-legal intricacies of the code, and therefore represent a point of centralization.¹¹²

Even the most impeccably designed DAOs will have a focal point, even if it is the slightest concentration of power. And whenever there is a disparity in power, no matter how minor, parties will seek to abuse it in the absence of a legal watchdog.

In a legal vacuum, DAOs cannot be expected to robustly handle disputes and governance problems on their own. It is clear that transactions on the blockchain network involving a sizable group of investors need a disinterested third-party to fairly resolve their disputes. This note explores three threshold questions that must be addressed before we jump to adjudication. The questions being: (1) What substantive rules should the neutral third-party use to adjudicate disputes from DAOs? (2) Which neutral third-party is best suited for this task? (3) And which parties ought to bring DAO smart contract disputes in front of a neutral third-party tribunal? This Note proposes that (1) the fiduciary duties of loyalty and due care from the law of corporations and the doctrine of public policy from the law of contracts should be applied (2) in the court system (3) by government regulatory bodies. To achieve this goal, a combination of efforts from the legislature and regulatory agencies would be needed.

¹¹¹ Voshmgir, *supra* note 24.

¹¹² *See id.*

A. *What to Enforce: Fiduciary Duties from Corporate Law and The Doctrine of Public Policy from Contract Law*

On the issue of what substantive rules should be applied to DAOs, this Note borrows rules and doctrines from two areas of substantive law: corporate law and contract law. This is because of the dual nature of DAOs; a DAO is a programmable contract that vests voting rights and rights to profits to its “shareholders.” This Note adopts the fiduciary duties of loyalty and due care as defined by state corporate law (e.g., Delaware General Corporate Law). This Note also supports the application of the well-established doctrine of public policy from contract law.

1. *The Fiduciary Duties of Loyalty and Due Care*

In a traditional corporation, “[d]irectors owe a duty of loyalty to the corporation . . . [that] both forbids directors to ‘stand on both sides’ of a transaction and prohibits them from deriving ‘any personal benefit through self-dealing.’”¹¹³ This has an effect of “mandat[ing] that a director not consider or represent interests other than the best interests of the corporation and its stockholders in making a business decision.”¹¹⁴ Directors also owe a duty of care in that they must exercise a “requisite degree of care in the process of decisionmaking and act on an informed basis.”¹¹⁵ Scholarship¹¹⁶ and the current practice of state courts¹¹⁷ also espouse the application of both fiduciary duties of loyalty and due care to non-corporate business entities such as limited liability companies.

The purported goal of DAOs is to successfully manage the assets under their control and to maximize their net economic returns. The manner in which DAOs achieve this may vary depending on their specific smart contract code, but they essentially follow the same script: investors entrust their cryptocurrency assets to a central administrator who manages the investments. Even in a DAO that has drastically attenuated the powers of the central administrator, some kind of

¹¹³ R. FRANKLIN BALOTTI & JESSE A. FINKELSTEIN, *BALOTTI AND FINKELSTEIN’S DELAWARE LAW OF CORPORATIONS AND BUSINESS ORGANIZATIONS* § 4.16 (3d ed. Supp. II 2019) (“The duty of loyalty also ‘encompasses cases where the fiduciary fails to act in good faith.’”).

¹¹⁴ *Id.*

¹¹⁵ *Id.* at § 4.15.

¹¹⁶ See Lyman Johnson, *Delaware’s Non-Waivable Duties*, 91 B.U. L. REV. 701, 702 n.6 (2011).

¹¹⁷ See *id.* at 2-3 n.8 (“In the absence of clear contractual language modifying or eliminating fiduciary duties, Delaware courts impose traditional fiduciary duties on managers and controlling members of LLCs. See, e.g., *Kelly v. Blum*, C.A. No. 4516-VCP, 2010 WL 629850, at *10 nn.69-70 (Del. Ch. Feb. 24, 2010).”).

centralization of power is unavoidable.¹¹⁸ Insofar as the central administrator possesses some kind of authority over the investors' assets, it can be said that the investor and the central authority have formed a fiduciary relationship.

i. The Duty of Loyalty

When parties form such a fiduciary relationship, it is difficult to contract *ex ante* for specific behavior of the fiduciary due to the inherent uncertainty of asset management.¹¹⁹ In addition, the cost of constantly monitoring the fiduciary is too high to be feasible.¹²⁰ Thus, in such a relationship, the beneficiary is exposed to a risk that the fiduciary may misappropriate the asset for his own benefit, but may not have sufficient information to determine whether the fiduciary has been acting in bad faith or not.¹²¹ Due to the beneficiary's imperfect information, the probability of the fiduciary receiving a sanction for his wrongdoing is less than 100%. However, if the sanction for the fiduciary's misappropriation were mere disgorgement of the asset, misappropriation would be profitable on average, and a fiduciary cannot be deterred from stealing.¹²² "Just as a thief cannot be deterred simply by requiring her to return the stolen goods whenever she is caught, [a fiduciary] cannot be deterred from appropriating the [beneficiary's] asset if the sanction is perfect disgorgement."¹²³ The fiduciary duty of loyalty is a bundle of rules designed to solve such a deterrence problem by raising the enforcement probability and increasing sanctions.¹²⁴ The duty of loyalty accomplishes this by imposing evidentiary rules (e.g., presumption of misappropriation, burden of proving a transaction's fairness on the fiduciary) — which raise the probability of enforcement—and punitive damages—which disincentivizes misappropriation because it requires more than mere disgorgement of the misappropriated asset.¹²⁵

Such legal burdens (in the form of penalties and harsh evidentiary burdens), however, may cause fiduciaries to "respond defensively by avoiding questionable conduct, ensuring that compliance with fiduciary rules is apparent and incontestable,

¹¹⁸ See Voshmgir, *supra* note 24.

¹¹⁹ See Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045, 1046-47 (1991).

¹²⁰ See *id.* at 1047.

¹²¹ When the only information revealed to the beneficiary is his poor returns, he cannot distinguish the fiduciary's misappropriation of the asset from the poor performance of the investment. See *id.* at 1051.

¹²² See *id.* at 1052-53.

¹²³ *Id.* at 1053.

¹²⁴ See *id.* at 1054.

¹²⁵ See *id.* at 1054-56.

and obtaining the consent of [the beneficiary] . . . for potentially suspect transactions.”¹²⁶ This will most likely “increase the fiduciary’s costs, reduce her productivity, and cause her to forego advantageous opportunities.”¹²⁷ To be economically justified, it is important for the specific rules in the fiduciary duty of loyalty to set a cost on fiduciaries that is less than the gain to beneficiaries from the decrease in wrongdoing by fiduciaries.¹²⁸ Neutral third-parties, tasked with adjudicating a DAO-related dispute, can rely on state corporate law to provide a rich background from which they can find laws on the duty of loyalty finely tuned to the economics of fiduciaries.

The fiduciary duty of loyalty should have its place in governing DAOs, even when the fiduciary’s powers and functions over a beneficiary’s assets are largely automated (and thus attenuated). As long as there exists some degree of centralization of power, which is inevitable,¹²⁹ a fiduciary can exert some degree of discretion over the beneficiary’s asset, and that leaves room for misappropriation. The stakes are high, especially when countless DAO-like entities are already raising monumental sums of money through initial coin offerings (“ICOs”), the sale of “coins” (similar to the sale of DAO Tokens) to investors to raise cryptocurrencies to be used in various projects on the blockchain. In 2017, “there were a total of 552 ICOs with a volume of just over \$7.0 billion.”¹³⁰ By mid-2018, “537 ICOs with a total volume of more than \$13.7 billion [had] been registered since the beginning of the year.”¹³¹ However, more than 80% of ICOs in 2017 were identified as scams.¹³² Formalizing and enforcing the fiduciary duty of loyalty in the blockchain world could begin to stem the prevalence of such deceitful schemes.

ii. The Duty of Due Care

Misappropriation of assets is not the only way in which a fiduciary can breach his duty; a fiduciary may manage the beneficiary’s assets carelessly. A fiduciary must make sound decisions on how to manage an asset by obtaining and relying on

¹²⁶ *Id.* at 1064.

¹²⁷ *Id.* at 1064-65.

¹²⁸ *Id.* at 1065.

¹²⁹ *See* Voshmgir, *supra* note 24.

¹³⁰ Markus Kasanmascheff, *PwC Report Finds That 2018 ICO Volume is Already Double That of Previous Year*, COINTELEGRAPH (June 30, 2018), <https://cointelegraph.com/news/pwc-report-finds-that-2018-ico-volume-is-already-double-that-of-previous-year>.

¹³¹ *Id.*

¹³² *See* Ana Alexandre, *New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams*, COINTELEGRAPH (July 13, 2018), <https://cointelegraph.com/news/new-study-says-80-percent-of-icos-conducted-in-2017-were-scams>.

relevant information.¹³³ The fiduciary duty of due care can also be seen as a bundle of rules, similar to the duty of loyalty, designed to incentivize a fiduciary to exercise diligence and care instead of shirking his responsibilities.¹³⁴

Unlike the duty of loyalty, which requires the fiduciary to give no weight to his own interests, the duty of care should not require unwavering diligence to the beneficiary at the excessive expense of the fiduciary.¹³⁵ This makes economic sense because the more effort the fiduciary expends in managing an asset, the marginal cost for the fiduciary goes up while the marginal value for the beneficiary goes down.¹³⁶ In this context, if a fiduciary operates at a level of effort where his marginal cost remains lower than the marginal benefit for the beneficiary, he can be said to be shirking his duties.¹³⁷ Thus, for optimal deterrence, the duty of due care should charge a grossly negligent fiduciary with compensatory damages greater than the cost that he is saving by shirking.¹³⁸

One may think that enforcing the duty of due care does not belong in DAOs. After all, many traditional processes requiring the diligence of the fiduciary can be either automated or delegated to investor vote in a DAO. However, no matter how trivial the effort, as long as there is some central authority exercising its diligent management over a DAO's assets, the duty of care is needed. Slock.it's curators could have been negligent in screening The DAO's proposals. A smart contract developer can be careless in programming a DAO's code. Enforcing the duty of due care will motivate fiduciaries in DAOs to exercise greater care and reduce human error in a field where even a small coding error can have dire consequences.

2. *The Doctrine of Public Policy*

Even with the fiduciary duties of loyalty and due care, it is still possible for DAOs to engage in illicit activity. Imagine a DAO that raises funds from investors to acquire drugs and sell them via the blockchain. Suppose that the smart contract code doesn't screen for age, making it possible for minors to purchase drugs. Imposing fiduciary duties will do nothing to prevent such criminal activity. The duties are designed to protect only the pecuniary interests of beneficiaries. After all, it could be said that the DAO was loyal to the profits of its investors and exercised due care in its transactions. The enforcement of the contract law doctrine of public

¹³³ See Cooter & Freedman, *supra* note 119, at 1056.

¹³⁴ See *id.* at 1056-61.

¹³⁵ See *id.* at 1059.

¹³⁶ See *id.* at 1058.

¹³⁷ See *id.* at 1059.

¹³⁸ See *id.* at 1059-60.

policy, stating that an agreement is unenforceable if it goes against legislation or it is clearly outweighed by public policy,¹³⁹ is necessary to deter DAOs from being used for unlawful purposes.

An online platform that goes against the law and public policy, albeit not a smart contract on blockchain, was shut down by the Department of Justice in 2013. “Silk Road was a massive, anonymous criminal marketplace that operated using the Tor Network, which renders Internet traffic through the Tor browser extremely difficult to trace.”¹⁴⁰ Originally founded on libertarian ideals, the marketplace quickly took a turn for the worse as its customers “principally bought and sold drugs, false identification documents, and computer hacking software.”¹⁴¹ Between 2011 and 2013, “thousands of vendors used Silk Road to sell approximately \$183 million worth of illegal drugs, as well as other goods and services.”¹⁴² The founder of Silk Road, Ross Ulbricht, was found guilty for narcotics trafficking, money laundering, computer hacking, and operating a criminal enterprise.¹⁴³

Another online enterprise, this time a blockchain smart contract, has recently caught the attention of the Commodities Futures Trading Commission (“CFTC”).¹⁴⁴ Augur is a blockchain-based prediction market platform which launched in July 2018.¹⁴⁵ Running on the Ethereum blockchain, “Augur allows anyone to create contracts to predict future events such as the outcome of basketball games, elections, the price of Bitcoin or the closing value of the Dow Jones Industrial Average.”¹⁴⁶ Bets and payouts are made using cryptocurrencies, and about \$1.5 million was wagered within the first two weeks of Augur’s launch. In many ways the distinction

¹³⁹ See RESTATEMENT (SECOND) OF CONTRACTS § 178 (AM. LAW INST. 1981); see also 17A C.J.S. *Contracts* § 278 (2019) (“Contracts contrary to public policy, that is, those which tend to be injurious to the public or against the public good, are illegal and void, even though actual injury does not result therefrom.”).

¹⁴⁰ *United States v. Ulbricht*, 858 F.3d 71, 82 (2d Cir. 2017).

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ See *United States v. Ulbricht*, 31 F. Supp. 3d 540, 546 (S.D.N.Y. 2014).

¹⁴⁴ See Matthew Leising, *As Crypto Meets Prediction Markets, Regulators Take Notice*, BLOOMBERG (July 26, 2018), <https://www.bloomberg.com/news/articles/2018-07-26/as-crypto-meets-prediction-markets-u-s-regulators-take-notice>.

¹⁴⁵ See Mike Orcutt, *This New Blockchain-Based Betting Platform Could Cause Napster-Size Legal Headaches*, MIT TECH. REV. (Aug. 2, 2018), <https://www.technologyreview.com/s/611757/this-new-ethereum-based-assassination-market-platform-could-cause-napster-size-legal/>.

¹⁴⁶ Leising, *supra* note 144.

between prediction markets and gambling is not clear,¹⁴⁷ and one problem with Augur is that it could be seen as an online gambling site, which is illegal under federal laws.¹⁴⁸ Even if the bets occurring on Augur were not interpreted to be gambling, they at least constitute either event contracts or binary options, which are both unlawful to list without approval from the CFTC.¹⁴⁹ CFTC Commissioner Brian Quintenz has recently remarked that the CFTC has generally prohibited prediction markets, where individuals use binary options or event contracts to bet on the outcome of future events, as against public policy.¹⁵⁰ Event contracts present an even more alarming problem than gambling. “[E]vent contracts based upon war, terrorism, assassination, or other similar incidents may be contrary to the public interest”¹⁵¹ because they present a financial incentive for event contract participants to actively engage in such activities. The CFTC has noted the resemblance of the Augur contracts to binary options and event contracts but has yet to pursue any action against Augur.¹⁵²

Smart contracts were conceived to facilitate transactions. But because the blockchain space operates on a pseudonym-basis and is less regulated than traditional markets, it is prone to spawn illegal transactions and markets that go against the public welfare. Enforcing the contract law doctrine of public policy can help DAOs stay true to their purpose, facilitating transactions without producing negative externalities.

*B. Which Neutral Third-Party Will Adjudicate: Courts, Arbitrators, or Blockchain Dispute Resolution Services*¹⁵³

The smart contract of The DAO appointed curators to oversee which project proposals would be selected and to act as caretakers of inactive token holders’ funds.¹⁵⁴ Despite creating a managerial position that had the potential to be heavily abused and create disputes, The DAO smart contract didn’t include any clause (or code) requiring the selection of a neutral third-party as a dispute resolution

¹⁴⁷ See Orcutt, *supra* note 145.

¹⁴⁸ See 31 U.S.C. § 5363 (2006).

¹⁴⁹ See Orcutt, *supra* note 145.

¹⁵⁰ See Brian Quintenz, Comm’r, U.S. Commodity Futures Trading Comm’n, Remarks at the 38th Annual GITEX Technology Week Conference (Oct. 16, 2018), <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>.

¹⁵¹ *Id.*

¹⁵² See Leising, *supra* note 144.

¹⁵³ This section will assume that jurisdictional issues have already been resolved.

¹⁵⁴ See JENTZSCH, *supra* note 25, at 2.

mechanism.¹⁵⁵ This Note has already established that self-driven governance and dispute resolution, especially in a legal void such as the blockchain space, will always be fruitless. There are three viable options for dispute resolution: courts, arbitration, and dispute resolution services, and this Note will determine which neutral third-party is best situated to resolve disputes of DAOs by applying the aforementioned corporate law and contract law doctrines.

1. *The Court System*

Perhaps the most defining characteristic of DAO-related disputes is their novelty. Although blockchain technology made its public debut in 2008 when the Bitcoin whitepaper was released, it didn't gather mainstream attention until around 2014 when users began to realize that the underlying technology could be utilized for applications other than cryptocurrencies.¹⁵⁶ With blockchain technology and smart contracts only being exposed to the public eye for about five years, the law didn't have much time to catch up with their technological developments. This Note proposes that the court system is best suited to adjudicate smart contract disputes, especially when there is a dearth of positive law and judicial opinions on the topic of smart contracts.

The greatest advantage the court system has over other neutral third-parties is its ability to generate precedent. “American courts follow the doctrine of *stare decisis* and defer to earlier cases on similar issues.”¹⁵⁷ *Stare decisis* confers many benefits on the American legal system such as predictability, efficiency, and legitimacy.¹⁵⁸ The court system's ability to set precedent is particularly valuable in an emergent area of law where there is no precedent to grant the above benefits. Even a single successful case of smart contract dispute resolution can provide a precious point of reference on which future courts and other tribunals can then rely.

When it comes to the first precedent-setting smart contract disputes, the adjudicating tribunal's primary concern should be the accuracy of the opinion. Accurate judgments require correctly applying the substantive law to the facts and

¹⁵⁵ *See id.*

¹⁵⁶ *See* Bernard Marr, *A Very Brief History of Blockchain Technology Everyone Should Read*, FORBES (Feb. 18, 2018), <https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/>.

¹⁵⁷ John M. Walker Jr., *The Role of Precedent in the United States: How Do Precedents Lose Their Binding Effect?*, STANFORD LAW SCH.: CHINESE GUIDING CASES PROJECT 2 (Feb. 29, 2016), <https://cgc.law.stanford.edu/wp-content/uploads/sites/2/2016/02/CGCP-English-Commentary-15-Judge-Walker.pdf>.

¹⁵⁸ *See id.* at 3.

technology of the case. There is no reason to doubt the court system's legal expertise. Judges are more than capable of not only navigating the rules making up the fiduciary duties of loyalty and due care, but also discerning what is in the public's interest for the purpose of the contract law doctrine of public policy. While there may be valid concerns about the court's subject matter expertise in a smart contract dispute, courts have ample resources to develop adequate insight into blockchain technology. Judges have access to expert witnesses brought into court by the litigants, and courts are flexible enough to arrange for technology tutorials prepared by said experts.¹⁵⁹ Furthermore, there already exists a degree of specialization in the modern court system, both at the state and federal levels.¹⁶⁰ If smart contract disputes become more prevalent, state and federal legislatures may foster subject matter expertise in smart contracts and blockchain technology by creating specialized courts. The appeals process also increases the likelihood of the court system delivering an accurate judgment.

Finally, the court system has finely calibrated rules of evidence and procedure to ensure fair process. A self-governed contractual dispute is prone to abuses of bargaining power. This can be seen in the example of The DAO where investors weren't given meaningful control in a vote to resolve a smart-contract dispute. The smaller investors in The DAO were disadvantaged by a lack of voting information and a voting system that disproportionately favors voters with more votes to spare. The court system's rules of evidence and procedure, on the other hand, are established and upheld by neutral judges with no stake in the smart contract dispute. Unless the parties contract around them, the rules do not bend to fit the purposes of one party over the other. This guarantees that a party with greater bargaining power is not unduly favored in the court system.

This is not to say that the court system is without flaws. Litigation in courts can be lengthy and expensive. The parties may not want to reveal the details of their dispute to the public. Such drawbacks, however, are secondary to the goal of establishing accurate precedent through a fair process, especially when no such precedential authority yet exists.

¹⁵⁹ *Markman* hearings in a patent infringement suit give federal district courts the discretion to entertain technology tutorials prepared by an expert. See J. Michael Jakes, *Using an Expert at a Markman Hearing: Practical and Tactical Considerations*, IP LITIGATOR (Aug. 2002, <https://www.finnegan.com/en/insights/using-an-expert-at-a-markman-hearing-practical-and-tactical.html>).

¹⁶⁰ See Chad M. Oldfather, *Judging, Expertise, and the Rule of Law*, 89 WASH. U. L. REV. 847, 847-48 (2012).

2. Arbitration

The number of federal civil cases resolved by trial between 1962 and 2002 has decreased by 84%.¹⁶¹ “This dramatic decrease in the trial rate may be attributed, at least in part, to business and public concerns about the high costs and delays associated with full-blown litigation, its attendant risks and uncertainties, and its impact on business and personal relationships.”¹⁶² Conventional wisdom suggests that arbitration addresses these concerns by offering lower costs, shorter resolution times, confidentiality, and a more flexible process.¹⁶³

Nevertheless, arbitration has a critical drawback as a dispute resolution mechanism that makes it incompatible with resolving smart contract disputes on DAOs. To the extent that arbitrators create precedent, it is unclear whether such precedent plays a meaningful role in guiding future disputes.¹⁶⁴ The Financial Industry Regulatory Authority (“FINRA”), which operates the largest securities dispute resolution forum in the United States, typically does not issue any explanations for their arbitration awards.¹⁶⁵ In a survey of National Association of Security Dealers (“NASD”) arbitration awards from the years 2003 and 2004,¹⁶⁶ “fewer than 5% of awards provided even a brief explanation for the result, and fewer than half of these included anything ‘that would be deemed an opinion by any stretch of the definition.’”¹⁶⁷ Surely securities arbitration awards, with such terse reasoning, would have very little, if any, precedential value. Other areas of arbitration, such as employment or class arbitration, do write reasoned awards, but they rely heavily judicial precedent and hardly consider arbitral precedent.¹⁶⁸ The literature has also suggested that even the parties to arbitration may not see arbitration awards as legitimate sources of legal authority.¹⁶⁹ As previously explained in Section IV.B.1,

¹⁶¹ See Thomas J. Stipanowich, *Arbitration: The “New Litigation,”* 2010 U. ILL. L. REV. 4 (2010).

¹⁶² *Id.*

¹⁶³ See *id.*

¹⁶⁴ See W.C. Mark Weidenmaier, *Judging-Lite: How Arbitrators Use and Create Precedent*, 90 N.C. L. REV. 1091, 1124-31 (2012).

¹⁶⁵ See *id.* at 1104.

¹⁶⁶ NASD combined with the member regulation, enforcement, and arbitration operations of the New York Stock Exchange to form FINRA.

¹⁶⁷ Weidenmaier, *supra* note 164, at 1104 (citing Jennifer J. Johnson, *Wall Street Meets the Wild West: Bringing Law and Order to Securities Arbitration*, 84 N.C. L. REV. 123, 144 (2005)).

¹⁶⁸ Only 1.3% of employment arbitration awards and 15.5% of class arbitration awards cite arbitral precedent. Labor arbitration is a curious outlier with 76.2% of its awards citing arbitral precedent. See Weidenmaier, *supra* note 164, at 1125.

¹⁶⁹ See *id.* at 1130-31.

respect for precedent is what gives the American judicial system its predictability, efficiency, and legitimacy.¹⁷⁰ The importance of precedent is accentuated in a field that has no established body of formal legislative or judicial guidance. Without the ability to create persuasive precedent, it is unlikely that arbitration will function well in adjudicating disputes arising from smart contracts.

3. *Blockchain Dispute Resolution Services*

By “blockchain dispute resolution service,” this Note refers to private dispute resolution services, which take the form of smart contracts that purport to manage disputes arising specifically from blockchain technology and smart contracts. Such services have been growing in number since cryptocurrencies gained mainstream popularity as an investment vehicle.¹⁷¹ The essential function of these services is to elect an online jury that will determine the outcome of the dispute by majority vote. The procedures through which these services select jurors varies wildly, from randomly choosing from those who have invested cryptocurrencies in the service¹⁷² to selecting from juror applicants pre-screened for legal experience.¹⁷³ Most blockchain dispute resolution services contemplate an incentive system where jurors not only receive an arbitration fee for their services, but also rack up a reputation score within the dispute resolution platform depending on the quality of their adjudications.¹⁷⁴ A higher reputation score will make the juror eligible for higher-stakes disputes and greater fees. One service proposes that all parties to a smart contract *ex ante* agree to deposit payments to an escrow account rather than make payments directly to the counterparty.¹⁷⁵ That service proposes guidelines for the timings of the deliveries of these payments to the escrow account and to the respective parties to the smart contract.¹⁷⁶

Blockchain dispute resolution services are still in development and some have obvious flaws in their inner workings. But, it is conceivable that a well-functioning product could result if one were to take the well-thought-out and redeeming qualities

¹⁷⁰ See Walker Jr., *supra* note 157.

¹⁷¹ JUR, WHITEPAPER: DECENTRALIZED DISPUTE RESOLUTION INFRASTRUCTURE (2019), <https://jur.io/wp-content/uploads/2019/05/jur-whitepaper-v.2.0.2.pdf>; JURIS PROJECT, WHITEPAPER: JUSTICIA USQUAM EX NUSQUAM (Sept. 18, 2018), <https://getjuris.com/publications>; CLEMENT LESEAGE & FEDERICO AST, KLEROS (Sept. 2019), <https://kleros.io/assets/whitepaper.pdf>.

¹⁷² See KLEROS, *supra* note 171, at 3.

¹⁷³ JURIS PROJECT, *supra* note 171, at 18-19.

¹⁷⁴ See *id.* at 40-46.

¹⁷⁵ JUR, *supra* note 171.

¹⁷⁶ See *id.* at 12.

from a variety of these services and combined them into a single service. This Note discusses blockchain dispute resolution services generally without limiting its analysis to any single service.

As articulated in Section IV.B.1 of this Note, a correct judgment requires both legal and subject matter expertise. The jurors for blockchain dispute resolution systems, compared to judges and arbitrators, would have unparalleled subject matter expertise on smart contracts. It can be presumed that the jurors, who are selected from users who have invested cryptocurrencies into the dispute resolution platform, possess at least a baseline understanding of how blockchains, cryptocurrencies, and smart contracts work. The same cannot be presumed for the jurors’ legal expertise; they cannot be expected to have even an iota of familiarity with fiduciary duties or public policy exceptions in contracts. Clever design of a blockchain dispute resolution service’s procedures can counteract the general lack of legal acumen amongst jurors to a certain extent, but these are imperfect solutions to a more fundamental problem. One particular service controls for its jurors’ lack of legal knowledge by pre-screening jurors for legal experience, but still permits laypeople to join in on the adjudication.¹⁷⁷ Another service has a procedure for appeals, but without any guarantee that the next panel of jurors will be any more qualified.¹⁷⁸ The court system spends extensive resources toward building up its judges’ subject matter expertise. Judges will have access to technology experts in the course of litigation. The court system is able to supply the time and expenses needed for judges to learn the requisite technical knowledge. Jurors of blockchain dispute resolution services, on the other hand, do not enjoy such support. A panel of jurors is not guaranteed to have a judge or other impartial legal professional to guide them. It is notably dubious whether blockchain dispute resolution services can adequately prepare their jurors to accurately adjudicate disputes, when they claim to issue decisions substantially faster and at a much lower cost than arbitration and litigation.¹⁷⁹

The three blockchain dispute resolution services studied by this Note do not contemplate the generation of precedent.¹⁸⁰ They do not identify what substantive body of law they will rely on as their guiding principle. Instead, two of the platforms, Jur and Kleros, envision the blockchain community coming up with substantive

¹⁷⁷ JURIS PROJECT, *supra* note 171, at 40-46.

¹⁷⁸ LESEAGE & AST, *supra* note 171, at 8.

¹⁷⁹ Jur claims that jurors will typically decide the most complex cases within 60 days. The simplest disputes are resolved for free within 24 hours. *See* JUR, *supra* note 171, at 31.

¹⁸⁰ *See* JURIS PROJECT, *supra* note 171; JUR, *supra* note 171; LESEAGE & AST, *supra* note 171.

guidelines about how to resolve disputes.¹⁸¹ The blockchain dispute resolution services have not yet specified the details of this suggested mock legislation. Even if we were to assume that such guidelines could eventually transform blockchain dispute resolution services into an efficient and predictable system, blockchain dispute resolution services are far from achieving that goal. In their current state, different blockchain dispute resolution services with different jurors would most likely diverge in their rulings for an identical dispute; the different services are akin to black boxes that spit out arbitrarily decided verdicts.

4. *The Unique Problem of Enforcement*

There is one attribute of the different neutral third parties that we haven't yet discussed—enforcement ability. How effectively can the different neutral third parties enforce their award of damages? Courts typically enforce civil damages awards by issuing a writ of execution.¹⁸² The writ empowers an enforcement officer to garnish the debtor's wages, bank account, or other assets.¹⁸³ Awards from arbitration and blockchain dispute resolution services can also be collected in the above manner by having a court confirm the award.¹⁸⁴

Smart contract disputes are unique because the disputes involve cryptocurrencies, which can be very difficult to retrieve. If a party is holding its assets on a widely used cryptocurrency exchange, a writ of execution could be sufficient to compel the exchange to surrender the relevant assets. Even if the assets were not retrievable from the cryptocurrency exchange, an enforcement officer could collect money by seizing other properties owned by the debtor. However, things become much more complicated if the debtor owns all of his assets as cryptocurrencies in an address that is privately held. In other words, only the debtor has the private key to his cryptocurrency “wallet” and consequently, only the debtor is able to withdraw his cryptocurrencies. This creates a difficult situation because the standard ways in which enforcement officers go about collecting payments aren't going to get them any closer to the cryptocurrencies. In such situations, courts can

¹⁸¹ See JUR, *supra* note 171, at 20; LESEAGE & AST, *supra* note 171, at 10.

¹⁸² See Fed. R. Civ. P. 69(a).

¹⁸³ See NEW YORK STATE UNIFIED COURT SYSTEM, COLLECTING THE JUDGMENT, (Apr. 1, 2013), <https://www.nycourts.gov/courts/nyc/civil/collectingjudg.shtml>; see also COLLECTION BASICS, NEW YORK STATE UNIFIED COURT SYSTEM (Mar. 14, 2018), <https://www.nycourts.gov/courthelp/AfterCourt/collectionBasics.shtml>.

¹⁸⁴ The language of the Federal Arbitration Act allows the appointment of blockchain dispute resolution services as arbitrators, provided that the parties agree by written contract. Parties to the arbitration may apply to a court to confirm arbitration awards. See 9 U.S.C. §§ 2, 9 (West 2018).

only incarcerate the disobeying party under a civil contempt charge until they comply with the court’s order.¹⁸⁵

Where courts and arbitrators would struggle to enforce a judgment involving cryptocurrencies, blockchain dispute resolution services provide a potential workaround for the problem. The blockchain dispute resolution services Kleros and Jur also provide escrow accounts in their smart contracts.¹⁸⁶ The Kleros and Jur escrow accounts can be opted into during contractual negotiations. Rather than making direct cryptocurrency payments to the other party at each contractual step, holding the payments in escrow and delaying delivery until the parties demonstrate further performance of the smart contract could circumvent difficult enforcement problems and hold-up problems. Protocols on smart contract design developed by blockchain dispute resolution services can serve as guidelines on how exactly to structure these transactions.¹⁸⁷

C. *Who Will Enforce: Private Investors or Government Regulatory Agencies*

The final question posed by this Note is which agent is in the best position to enforce the law on otherwise unregulated disputes in DAOs. This Note has identified two categories of litigants that can potentially meet the challenge: private investors to the smart contracts and government regulatory agencies.

1. *Private Investors*

Before we inquire into the legal options that private actors can pursue against self-governed DAOs, it is important to identify who the average private investor is. Although there is some variance between survey results, they all seem to agree that the average cryptocurrency holder is male, millennial (between 18 and 39 years of age), and middle class (income of \$50,000 to \$100,000 a year).¹⁸⁸

¹⁸⁵ Philip Moustakis, Lecture at New York University Stern School of Business (Mar. 27, 2019).

¹⁸⁶ See JUR, *supra* note 171, at 12; Stuart James, *Kleros Escrow Explainer—Secure Your Blockchain Transactions Today*, KLEROS (Apr. 30, 2019), <https://blog.kleros.io/kleros-escrow-secure-your-blockchain-transactions-today>.

¹⁸⁷ See JUR, *supra* note 171, at 12-14.

¹⁸⁸ See Paul R. La Monica, *The Average Bitcoin Investor Really Is Young, Rich and Male*, CNN BUS. (Oct. 5, 2018), <https://www.cnn.com/2018/10/05/tech/bitcoin-investors-survey/index.html>; Kari Stray, *Bitcoin Users: Who They Are and What They Do?*, COINTELEGRAPH (Aug. 1, 2017), <https://cointelegraph.com/news/bitcoin-users-who-they-are-and-what-they-do>; Bloomberg, *This Is What the Average Bitcoin Owner Looks Like*, FORTUNE (Jan. 24, 2018), <https://fortune.com/2018/01/24/young-men-buying-bitcoin>.

With their relatively modest means, it is improbable that individual private investors will be able to bring large-scale smart contract disputes to court. Burbank, Farhang, and Kritzer have made the following observations while assessing private enforcement regimes:

In the absence of public legal aid or a private interest group champion, the poor and those of modest means who wish to initiate civil litigation require other forms of assistance in order to gain access to the market for legal services. Since the turn of the twentieth century, clients and lawyers have been free to contract for a no-win, no-fee representation. . . . Such arrangements are most common in, but not restricted to, tort litigation and they most commonly call for the lawyer to receive one-third of any monetary judgment. It is also typical of such arrangements that the lawyer will pay the costs of litigation, subject to full or partial reimbursement in the event of success. . . . [However,] [t]he opportunity to earn a contingent fee is unlikely to attract lawyers unless there is a reasonable prospect for a substantial monetary recovery. . . . As the cost of litigation has increased, two phenomena may have enhanced the importance of litigation-funding mechanisms that permit clients and their attorneys to look elsewhere than the clients' personal assets to fund legal representation. First, some of what was affordable litigation for fee-paying clients 40 or 50 years ago may no longer be, at least in federal court, with the result that those at risk of being denied access to the market for legal services are not just the poor and those of modest means but a larger segment of the middle class.¹⁸⁹

There are no public or private interest groups offering to fund litigation over smart contract disputes. Smart contract disputes have no precedent in the court system, and prospects for monetary recovery would be highly speculative at best. Even if investors sought to lower costs by consolidating their legal efforts, this is unlikely to be feasible since the investors will most likely be too dispersed and limited in their ability to communicate with each other.

There is another roadblock discouraging private investors from bringing smart contract disputes to court: it is unclear whether there are any private rights of action, express or implied, through which the private investors can claim relief. Unlike shareholder derivative suits in the corporate context, where the shareholders' claims and procedures are well defined, there is no legislation or case law that outlines what

¹⁸⁹ Stephen B. Burbank et al., *Private Enforcement*, 17 LEWIS & CLARK L. REV. 637, 653-54 (2013).

claims a plaintiff can bring in a dispute with a DAO. Considering that the Arizona and Tennessee legislatures enacted legislation acknowledging the legality of smart contracts, private investors may be able to bring contract law claims in those jurisdictions.¹⁹⁰ Even in those jurisdictions, however, private investors would have difficulty enforcing fiduciary duties onto DAOs.

2. Government Regulatory Agencies

Government agencies such as the SEC and the Commodity Futures Trading Commission (“CFTC”) have been fairly active in exercising oversight in the blockchain space. “[I]n early February 2018, the Chairman of the SEC and the Chairman of the CFTC both testified at a [Senate] hearing . . . entitled ‘Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission.’”¹⁹¹ The testimony demonstrated the continued collaboration and commitment of the two agencies to enforce the law on the blockchain.¹⁹² This Note presents enforcement actions by the SEC and CFTC addressing problems most analogous to those articulated by this Note.

On September 11, 2018, the SEC issued the Crypto Asset Management Order, “finding that the manager of a hedge fund formed for the purpose of investing in digital assets had improperly failed to register the fund as an investment company.”¹⁹³ The SEC also classified the fund's manager as an investment adviser, and found that he violated the antifraud provisions of the Investment Advisers Act of 1940 by making misleading statements to investors in the fund.¹⁹⁴

On January 24, 2018, the CFTC announced an enforcement action against the operators of My Big Coin (“MBC”), a cryptocurrency, alleging commodity fraud

¹⁹⁰ See ARIZ. REV. STAT. ANN. § 44-7061 (2017); TENN. CODE ANN. § 47-10-202 (West 2018).

¹⁹¹ J. Dax Hansen et al., *More Legal Aspects of Smart Contract Applications*, PERKINS COIE 13 (Mar. 2018), <https://www.perkinscoie.com/images/content/1/9/v3/199672/2018-More-Legal-Aspects-of-Smart-Contract-Applications-White-Pa.pdf>.

¹⁹² See *id.*

¹⁹³ *Statement on Digital Asset Securities Issuance and Trading*, U.S. SEC. AND EXCH. COMM’N (Nov. 16, 2018), <https://www.sec.gov/news/public-statement/digital-asset-securites-issuance-and-trading>.

¹⁹⁴ The misleading statements, however, were that the fund was regulated by the SEC and that the fund had filed a registration statement with the agency. See *SEC Charges Digital Asset Hedge Fund Manager With Misrepresentations and Registration Failures*, U.S. SEC. AND EXCH. COMM’N (Sept. 11, 2018), <https://www.sec.gov/news/press-release/2018-186>.

and misappropriation.¹⁹⁵ The defendants allegedly misappropriated over \$6 million from investors “by, among other things, transferring customer funds into personal bank accounts, and using those funds for personal expenses and the purchase of luxury goods.”¹⁹⁶

The SEC’s and CFTC’s enforcement actions are certainly steps in the right direction. They were, however, focused on prosecuting failures to register a venture with an agency (e.g., failures to register a security, an exchange, or a commodity) or blatant misrepresentations and frauds. The governance issues of DAOs that this Note seeks to address are more subtle and harder to detect but can have equally disastrous consequences. The real problem highlighted by The DAO incident isn’t the hacking attack that led to The DAO’s downfall; it’s the allegedly self-governing power structure within The DAO that, in reality, gave its investors no meaningful control over the entire enterprise and left them open to manipulation and exploitation. Government regulatory agencies, with their greater resources and expertise, should affirmatively investigate the suspect governance structures of DAOs and similar entities.

CONCLUSION

In the February 26, 1995 issue of *Newsweek*, American astronomer and author Clifford Stoll illustrated his skepticism of the Internet:

After two decades online, I’m perplexed. It’s not that I haven’t had a gas of a good time on the Internet. I’ve met great people and even caught a hacker or two. But today, I’m uneasy about this most trendy and oversold community. Visionaries see a future of telecommuting workers, interactive libraries and multimedia classrooms. They speak of electronic town meetings and virtual communities. Commerce and business will shift from offices and malls to networks and modems. And the freedom of digital networks will make government more democratic.

Baloney. Do our computer pundits lack all common sense? The truth in no online database will replace your daily newspaper, no CD-ROM can

¹⁹⁵ See *CFTC Charges Randall Crater, Mark Gillespie, and My Big Coin Pay, Inc. with Fraud and Misappropriation in Ongoing Virtual Currency Scam*, U.S. COMMODITY FUTURES TRADING COMM’N (Jan. 24, 2018), <https://www.cftc.gov/PressRoom/PressReleases/pr7678-18>.

¹⁹⁶ *Id.*

take the place of a competent teacher and no computer network will change the way government works.¹⁹⁷

Like the Internet back in the 1990s, blockchain technology is poised to change the world. Smart contracts have great potential to reduce costs for financial transactions. DAOs have the capacity to engender business entities that greatly simplify and automate traditional institutional governance regimes. Like any revolutionary invention, however, these nascent technologies will have to endure suspicions and growing pains before adoption by the greater society.

One such growing pain is the prevalence of fraud in the blockchain community. Despite the booming interest in blockchain technologies—the total market capitalization for cryptocurrencies peaked at \$795 billion in January 2018—shady dealings abound.¹⁹⁸ While studies disagree on the extent to which ICOs fail to deliver, the consensus seems to be that the typical ICO investment performs extremely poorly.¹⁹⁹ In addition, 78% of ICOs have been identified as scams.²⁰⁰

There is a lack of legislative and judicial oversight in the blockchain space. In such a legal vacuum, organization-like smart contracts, or DAOs, have resorted to resolving governance disputes on their own. This Note, through a case study of The DAO and review of economics literature, posits that self-governance of DAOs will ultimately result in misgovernance. Legislative, judicial, and regulatory bodies should work in tandem to affirmatively police the questionable governance practices of DAOs and enable an otherwise revolutionary technology.

¹⁹⁷ Clifford Stoll, *Why the Web Won't Be Nirvana*, NEWSWEEK (Feb. 26, 1995), <https://www.newsweek.com/clifford-stoll-why-web-wont-be-nirvana-185306>.

¹⁹⁸ *Global Charts*, COINMARKETCAP, <https://coinmarketcap.com/charts> (last visited Sept. 22, 2019).

¹⁹⁹ See Ana Alexandre, *Research: ICO Market Down Almost 100% From a Year Ago, Raised \$40 Million in Q1 2019*, COINTELEGRAPH (May 13, 2019), <https://cointelegraph.com/news/research-ico-market-down-almost-100-from-a-year-ago-raised-40-million-in-q1-2019>; U.S. COMMODITY FUTURES TRADING COMM'N, *supra* note 195; Sabrina T. Howell et al., *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales*, EUROPEAN CORP. GOVERNANCE INST. 1, 27 (2018), https://ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf

²⁰⁰ See Alexandre, *supra* note 199 (citing SHERWIN DOLAT, CRYPTOASSET MARKET COVERAGE INITIATION: NETWORK CREATION, 24 (July 11, 2018)).