Washington University Law Review

Volume 96 | Issue 3

2018

A Lawyer's Divorce: Will Decentralized Ledgers and Smart Contracts Succeed In Cutting Out the Middleman?

Charlotte R. Young
Washington University School of Law

A LAWYER'S DIVORCE: WILL DECENTRALIZED LEDGERS AND SMART CONTRACTS SUCCEED IN CUTTING OUT THE MIDDLEMAN?

INTRODUCTION

Society is progressing at a rapid pace. As math and science evolve, new technologies begin to utilize these advances and create something novel. These technological changes are revolutionizing not only the science-oriented industries, but also the humanities. One such example falls within the legal arena. More specifically, the exciting advent of smart contracts and their use of technological changes are altering the way law is processed and practiced.[1] However, as is often the case, new technological innovations spur certain growing pains. The implementation of smart contracts is proving no different.

Some view the smart contract as the start of a more ideal society.[2] With the aid of smart contracts and blockchain technology, machines can finally be equipped to fulfill some of the most basic human functions.[3] Not only would business transactions always occur in a timely, seamless, and cost-effective manner, but also more mundane life tasks, such as ordering laundry detergent,[4] could soon be done via smart contract technology. As

1. *See infra* note 4.
2. *See, e.g.*, Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [https://perma.cc/PV8D-RELV].
3. *Id.*
4. This is just one example of how smart contracts could revolutionize the way our society operates. Under this example, the owner of the washing machine and the store would enter into a contract prior to any required transaction. This contract would say something like: "If the volume of my laundry detergent falls below *X* level, then charge me for *X* amount of laundry detergent. If payment is successful, then send me *X* amount of laundry detergent. I authorize you to charge my card for the purchase of new detergent every time my washing machine sends you a notification detergent is needed." After forming this type of contract, Szabo's idea for smart property required some kind of mechanism to be embedded inside the washing machine itself. This mechanism would send the signal to a designated store each time the detergent fell below the specified threshold. In following the simple "if, then" style, the code to enact the smart contract would say "if the detergent falls below one ounce, then order a new bottle shipped from *X* store." In this example, a smart contract could eliminate a consumer's likelihood of ever running out of laundry detergent. By cutting out the middleman, the smart contract, operating within the washing machine itself, would be preauthorized to order detergent when necessary. Thus, this eliminates a consumer's need to ever monitor their levels of detergent. The desirability of such technology becomes apparent when applied to other aspects of life. *See infra* note 14 and accompanying text (discussing this technology as applied to the typical "repo man" business model). For more information regarding Szabo's idea of Smart Property and a current example of something similar to smart property, see *infra* note 14.

exciting as these changes may be, smart contracts and the blockchain technology behind them are still immature.[5] Before this legal phenomenon is widely accepted, there needs to be more advancement in not only the code that creates the technology, but also in the law and its regulations.[6] As it stands today, smart contracts are most likely to be accepted only in part, and heavily tailored to meet each contracting party's needs.

This Note will start by giving an overview of the technology needed to implement smart contracts—blockchain technology[7]—and an explanation of how smart contracts fit within the framework of a blockchain. Next, this Note will discuss some of the major issues smart contracts face. Such issues include: the need to translate natural language into computer code, the traditional concept of contracting in conjunction with the effect of smart contracts on traditional legal notions, and reoccurring enforcement issues. After discussing smart contracts and the current issues barring wide-spread acceptance, this Note will explore the future of smart contracts in the legal arena by analogizing such an electronic contracting change to the now-widely accepted electronic clickwrap agreements. Additionally, this Note will explore recently enacted state statutes that create favorable legal conditions for smart contracts and what impact, if any, these statutes may have upon federal legislation. Furthermore, this Note will analyze the lack of and potential need for regulations regarding smart contracts. In an attempt to make smart contracts acceptable, this Note will suggest future regulations focus on two components of smart contracts. As it will be discussed, regulations should require smart contracts to utilize a permissioned ledger and focus on ensuring the legal requirement of mutuality between the two contracting parties. Lastly, this Note will conclude that although the publicity surrounding smart contracts is exciting and innovative, this form of contracting is likely to remain in a controlled business environment with implementation under select circumstances.

5. Daniel Cawrey, *Why Ethereum Needs 'Dumb' Contracts*, COINDESK (June 29, 2016, 6:50 PM), https://www.coindesk.com/ethereum-dao-dumb-smart-contracts [https://perma.cc/Q2BS-6XCL].

6. *See infra* Part II.D (highlighting coding failures that have allowed hackers to breach blockchain security); *infra* Part VI (explaining the need for federal regulation of smart contracts to minimize parties' risks).

7. Blockchain is a type of decentralized ledger technology. *See infra* Part II.C (explaining how blockchain technology works). Although there is much debate concerning the appropriate terminology for blockchain/decentralized ledger technology, for the remainder of this Note, the two are considered synonymous. Hereinafter decentralized ledger technology will be referred to as blockchain.

I. Overview of the Technology

A. What is a smart contract?

There is no universally accepted definition of a smart contract.[8] In the mid-1990s, the general concept of a smart contract was broadly construed.[9] For this reason, the smart contract can hold a variety of nuanced meanings.[10]

Nick Szabo, widely recognized as the creator of the smart contract concept,[11] defined a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[12] The key focus in this definition is on the idea of new technology. For widespread use, Szabo believed that smart contracts needed to be embedded within the world.[13] In order to embed these smart contracts, Szabo suggested placing contractual clauses within everyday pieces of hardware, such as cars.[14] This could be done by designing a smart contract

8. Jenny Cieplak & Simon Leefatt, *Smart Contracts: A Smart Way to Automate Performance*, 1 GEO. L. TECH. REV. 417, 417 (2017). For a comprehensive list of features smart contracts encompass, see J. DAX HANSEN & CARLA L. REYES, PERKINS COIE LLP, LEGAL ASPECTS OF SMART CONTRACT APPLICATIONS 3 (2017) [https://perma.cc/5WUK-TK4V].

9. *See* NORTON ROSE FULBRIGHT, CAN SMART CONTRACTS BE LEGALLY BINDING CONTRACTS? 1 (2016) [https://perma.cc/MQN6-JYEM] (finding Szabo's original idea for smart contracts rather broad).

10. *Id.* at 4.

11. Cieplak & Leefatt, *supra* note 8, at 418.

12. Szabo, *supra* note 2. Additionally, Szabo noted that smart contracts were made possible because of the advances in digital technology. He was careful to state that smart contracts did not imply the use of artificial intelligence; rather, he coined the term "smart" because they were more functional than the traditional paper-based contracts. *Id.* For an example and further understanding on how a more complex smart contract operates, *see infra* Part II.D.

13. Szabo, *supra* note 2.

14. *Id.* Within the same paper, Szabo also proposed the idea of smart property. This is a more technologically advanced concept that runs parallel to smart contracting. Instead of embedding a smart contract within the software or hardware, a mechanism is physically placed within the object itself. A smart contract is what governs this physical mechanism. For example, Szabo suggested using the smart property concept to govern simple tasks such as loan payments on a new car. In this case, the mechanisms and smart contracts embedded in the car would determine whether monthly car payments are met. If not met, the contractual clause would automatically invoke a lien on the car, which would return legal possession of the car to the bank, and lock out the debt holder. Thus, with the exception of the bank, all access to the car would be restricted. The bank would then have the legal right to repossess the car. Typically, this task has been completed by a repossession agent (commonly known as a "repo man"). Perhaps in a more futuristic and technologically-advanced world, the failure to make appropriate payments could invoke a car's embedded smart contract and send the self-driving car back to its rightful legal owner (the bank). The benefits of smart property are cost effectiveness: Szabo believed that this smart property (in the former example "smart lien") would be cheaper than a repo man. The aforementioned example is a useful way to conceptualize smart contracts and their potentially monumental impact on our society. See *id.* for more discussion of smart property. Additionally, Amazon has recently unveiled a new concept, Amazon Dash Replenishment Service ("DRS"). Although DRS is similar to the idea of smart property, the DRS does not operate on a blockchain nor does it utilize a smart contract. The DRS is a modern example of how concepts, sparked by smart contracts and blockchain,

that utilized computer software to decipher the contract's parameters. The computer software would only allow a smart contract to be executed if the initial input conditions were met.[15] For this reason, a smart contract is comprised of simple "if, then" contractual clauses written into whatever technological platform is used to complete the transaction.[16] Szabo recognized that contractual breaches were a major issue impeding the advancement of business transactions. Therefore, the goal behind a smart contract was to embed, within the software and hardware, contractual clauses that make it difficult and expensive for a party to breach the agreement.[17] Because of the novel technology used to create a smart contract, Szabo considered smart contracts more advanced than their "inanimate paper-based ancestors."[18]

are moving closer to revolutionizing our way of life. *See*, *Dash Replenishment Service*, AMAZON, https://developer.amazon.com/dash-replenishment-service [https://perma.cc/YS52-JUMG]. *See also*, Michelle Evans, *Machines Will Know What You Need to Buy, But Are Retailers Ready?*, FORBES (Jul 11, 2018, 11:26 AM), https://www.forbes.com/sites/michelleevans1/2018/07/31/machines-will-know-what-you-need-to-buy-but-are-retailers-ready [https://perma.cc/G2JZ-DVZH] (describing upcoming changes to the retail market which mimic the smart property idea); *Wagz Integrates Amazon Dash Replenishment into new Serve Smart Feeder that Automatically Reorders and Ships Pet Food Right to Your Door*, CISION PR NEWSWIRE (May 23, 2018, 7:40 AM), https://www.prnewswire.com/news-releases/wagz-integrates-amazon-dash-replenishment-into-new-serve-smart-feeder-that-automatically-reorders-and-ships-pet-food-right-to-your-door-300653490.html [https://perma.cc/X79C-KPGZ] (although not operating on blockchain, this provides an example of a self-ordering pet food bowl, which mimics Szabo's idea of smart property).

15. *See* NORTON ROSE FULBRIGHT, *supra* note 10, at 7 (using a vending machine as an example to show that once coins are submitted, the smart contract enacts predetermined and irrevocable outcomes).

16. For a more complete discussion of preexisting technology that could easily utilize a smart contract, see Szabo, *supra* note 2. In 1996, Szabo suggested that the following types of technology could benefit from a smart contract: Point of Sale terminals and cards, Electronic Data Interchange used predominantly for transactions between corporations, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT), Automated Clearing House (ACH), and FedWire to transfer and clear payments between banks. More recently, many other forms of technology can, and will soon, benefit from the use of blockchain technology. *See* Lucas Mearian, *Blockchain will be the killer app for supply chain management in 2018*, COMPUTERWORLD (May 8, 2018, 2:55 PM), https://www.computerworld.com/article/3249252/emerging-technology/blockchain-will-be-the-killer-app-for-supply-chain-management-in-2018.html [https://perma.cc/44VF-PXFF] (discussing blockchain technology and its advantages to the global shipping industry and overall supply chain management); Hugo Evans & Stephen Easton, *The Future of Procurement Arrives at Last*, ATKEARNEY, https://www.atkearney.com/procurement/article?/a/the-future-of-procurement-arrives-at-last [https://perma.cc/W797-QLK4] (discussing the rationales and need for blockchain technology in the procurement process).

17. Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997) [https://perma.cc/4GN9-Q48G].

18. Szabo, *supra* note 2. Szabo frequently used the vending machine as an example of a "primitive ancestor of [a] smart contract[]." *Id.* A vending machine revolves around the smart contract concept because the machine takes the input (the coins), determines when the appropriate amount is rendered, and then uses a simple mechanism to digest the coins and deliver the product (the soda). Although the vending machine is similar to smart contracts in its overall concept (both operate on simple "if, then" scenarios), it is more rudimentary in key aspects. A smart contract usually entails synchronous steps involving multiple parties. Unlike a typical smart contract, the vending machine is only concerned

Although the smart contract concept can have many different definitions, Szabo's ideas spurred scholarship that eventually reached a consensus regarding key characteristics of any smart contract. For one, a smart contract is always in digital form and contains embedded contractual clauses.[19] Normally, these contractual clauses are written in the form of computer code. Additionally, the performance of a smart contract is always mediated by technology.[20] This means that payments and other actions within the contractual clauses are governed by rules-based operations on technological platforms. Essentially, there is no longer a need for the middleman. Furthermore, smart contracts are meant to be irrevocable.[21] Once a stipulated condition is met, the performance encoded within the smart contract cannot be stopped.[22]

B. How Blockchain and Smart Contracts Coexist

The recent invention of specialized technology has made smart contracts possible.[23] However, this was not always the case. Szabo's concept of smart contracts remained in the beta stage from the mid-1990s until the invention of the first digital coin, Bitcoin, in 2008.[24] The growing interest in Bitcoin and the technology on which it was built—blockchain—ignited numerous research and development projects regarding its practical application.[25]

---

with one relationship—the relationship between the vending company and the customer. Thus, the vending machine is a prime example of how a simple "if, then" smart contract operates. *Id.*

19. *Id.*

20. NORTON ROSE FULBRIGHT, *supra* note 10, at 7.

21. *Id.* A smart contract's irrevocability is the most controversial characteristic, perhaps, because this feature is a grave departure from traditional contracting. Although traditional contracts were created with the purpose of lasting, lawsuits and judicial interpretation could always create an "easy out," if desired. However, no such "easy out" exists with smart contracts. Instead, everything is automated behind the scenes with new and rapidly evolving technology. *Id.* Perhaps some of the fear surrounding smart contracting stems from a level of discomfort that tends to surface when dealing with new and not-fully-understood technology. Thus, the irrevocability characteristic makes smart contracts permanent; whereas, traditional contracting is only permanent when both parties desire it. This combination of new technology and permanency creates controversy.

22. *Id.*

23. *See supra* Part I.A.

24. NORTON ROSE FULBRIGHT, *supra* note 10, at 8. *See also* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/3U88-DR68].

25. *See* HANSEN & REYES *supra* note 8, at 3 (describing a smart contract's broad definition and hypothesizing that technologists and businesses will find new and revolutionary ways to use smart contracts and their encompassing technology). It is important to note the blockchains used for Bitcoin and Ethereum operate in two different manners. Under Bitcoin, the blockchain is being used to support a digital currency. However, under Ethereum, the blockchain is being used to run an open-ended decentralized software platform. It is because of this flexible platform that Ethereum, but not Bitcoin, is able to support smart contracts. *See* Prableen Bajpai, *Bitcoin Vs Ethereum: Driven by Different Purposes,*

Blockchain is the checking mechanism that facilitates and verifies transactions. Because of its versatility, blockchain can easily be adapted to verify any transaction, so long as it is translated into computer code. Two key features of smart contracts include automation and self-regulation via technology.[26] Smart contracts were able to obtain these features through the use of blockchain. Because blockchain acts as a checking mechanism, this self-regulation removes the human element, commonly referred to as the middleman. This removal has the benefit of streamlining the contracting process, lowering the likelihood of human error, and creating a more cost-effective option.[27]

Assuming all preliminary conditions are met, the machine using a smart contract will ensure performance on the contract's terms.[28] However, just like in traditional contracting, the initial terms of a smart contract must be interpreted and verified.[29] In traditional contracting, this is done by a human or, in some cases, a judge. Unlike traditional contracting, smart contracts utilize the third-party computer-based process, blockchain, to verify the occurrence of a contract's terms.[30]

C. A General Discussion on Blockchain Technology

As mentioned above, blockchain is a necessity for any smart contract. For that reason, this Note requires a brief discussion on the technology and how it operates.

Blockchain contains a decentralized ledger that anonymously tracks and creates a record of transactions pertaining to that ledger.[31] A block is created for each transaction. The ledger is responsible for containing a complete and continuous record (the "chain") of all transactions.[32] Each transaction equates to a "block;" however, these blocks are only added to the blockchain if the "nodes" reach a consensus that the block (the transaction) is valid.[33]

INVESTOPEDIA (July 13, 2018 6:00 AM), https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp [https://perma.cc/W3WZ-CFMZ].

26. *See supra* Part I.A.

27. Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 316 (2017). *See also* Cieplak & Leefatt, *supra* note 8, at 420.

28. Raskin, *supra* note 27, at 316.

29. *Id.* at 322.

30. HANSEN & REYES, *supra* note 8, at 2.

31. Cieplak & Leefatt, *supra* note 8. *See also* HANSEN & REYES, *supra* note 8, at 2.

32. JOHN MCKINLAY ET AL., DLA PIPER, BLOCKCHAIN: BACKGROUND, CHALLENGES, AND LEGAL ISSUES 5 (2017), https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/ [https://perma.cc/955V-9FAX].

33. *Id.*

One of the most notable features of a blockchain is its ability to exist simultaneously across a network of computers.[34] In order to record and check the accuracy of each transaction within the blockchain, the ledger must be replicated and distributed among multiple parties.[35] These parties, commonly referred to as "nodes,"[36] are often anonymous third-party members of the blockchain network.[37] The process of checking a transaction's validity requires a high level of computing power: "'miner' nodes compete with each other to solve a highly complex algorithm'"[38] which, if proven, will verify the transaction's validity.[39] The first miner node to solve the algorithm, thus verifying the transaction's validity, is rewarded.[40] Each block usually contains the following four pieces of information: a "hash" from the previous block, a summary of the actual transaction, a time stamp, and the verification of the transaction.[41]

Additionally, the blockchain network is decentralized, which has the primary benefit of making the technology hard to hack by eliminating the one centralized point of vulnerability.[42] Because blockchain lacks a centralized point, the ledger needs to be self-maintaining.[43] This is possible, in part, because each block contains the hash of the previous block.[44] This means that each current block is tied to the previous one, making any attempt by hackers to alter the transaction post-validation easily detected.[45]

Despite the lack of diversity in terms of a technological platform, a party to a smart contract still maintains choices regarding the design of the blockchain technology. Smart contracts can utilize a permissionless or permissioned ledger, or a hybrid of the two.[46] A permissionless distributed

34. *What is Blockchain Technology? A Step-By-Step Guide for Beginners*, BLOCKGEEKS, https://blockgeeks.com/guides/what-is-blockchain-technology/ [https://perma.cc/P54D-T2X9].

35. Cieplak & Leefatt, *supra* note 8, at 420–21. Either the entire ledger or parts of the ledger can be distributed to nodes. The choice depends on whether only certain portions are relevant to certain nodes. Either way, the distributed copy is still considered the original. This is because rules require all modifications or changes to the ledger (i.e. an asset changing hands or a transaction being created or modified) to be broadcasted to all existing copies of the ledger. *See id.* at 421.

36. For a helpful diagram of how blockchain works, see *supra* note 34; MCKINLAY ET AL., *supra* note 32, at 6. For an illustrative example using the a blockchain process, see *Smart Contracts*, BLOCKCHAINHUB, https://blockchainhub.net/smart-contracts/ [https://perma.cc/FUG9-5MAY].

37. MCKINLAY ET AL., *supra* note 32, at 5.

38. *Id.*

39. If utilizing Bitcoin's Blockchain, this is called the "proof of work." *Id.*

40. Again, if this is on Bitcoin's Blockchain, then such a miner node will be compensated in Bitcoin. For this reason, this action has also been referred to as "mining for Bitcoin." *Id.*

41. *Id.* at 7.

42. *Id.*

43. *Id.*

44. *Id.* at 5.

45. *Id.*

46. NORTON ROSE FULBRIGHT, *supra* note 10, at 11. It is also important to note that a party may "choose" whether the status of the contract is legally binding or legally enforceable. Although the Norton

ledger allows anyone "to download the software, submit messages for processing and/or be involved in the process of authentication, verification and reaching consensus."[47] Permissionless distributed ledgers are open to anyone and usually lack a designated leader.[48] Typically, this type of ledger utilizes blockchain's public proof-of-work method.[49]

Unlike the permissionless ledger, a permissioned ledger is private. The participants in a permissioned ledger must be either pre-selected, approved by an administrator of the ledger, or granted entry once the participant satisfies certain requirements.[50] Unlike the public proof-of-work method typically used in permissionless ledgers, permissioned ledgers make use of either a consensus protocol, an administrator, or sub-group of participants when deciding whether to update the ledger.[51] Thus, permissioned ledgers, in contrast to permissionless ledgers, contain a feature resembling a centralized body.[52]

A third alternative to the permissionless or permissioned ledger is to create a hybrid of the two, which can incorporate a variety of variables. Usually these variables relate to the level of centralization within the ledger.[53] For example, a hybrid ledger can stem from a permissionless-type ledger that opts to use an encryption code to protect the transactions.[54] Such a hybrid allows anyone to download the ledger; however, only those with a

---

Rose Fulbright White Paper implies that a party actually has a choice in the contract's legality, in reality, it is generally a choice of whether or not to add an arbitration clause. Because arbitration clauses are still subject to the discretion of a court for enforcement, this option may help the enforceability of a smart contract but it does not offer a concrete method ensuring the contract's enforceability. Additionally, a party may have a choice as to the "consensus protocol over which participants reach agreement over facts." *Id.* However, this option is more of an issue for the technologists because it pertains to the code utilized. Therefore, this Note will not discuss this option any further.

47. *Id.*

48. *Id.* The permissioned ledger, or some form of a hybrid, will likely be the preferred ledger for corporations and business transactions. Unlike a permissionless ledger, permissioned ledgers offer heightened security and anonymity that is more conducive to confidential and sensitive business dealings. *Id.* at 12.

49. *Id.* at 11. Essentially, proof-of-work is the term for the process through which blockchain technology verifies transactions. In layman's terms, proof-of-work is defined as "a requirement that expensive computations . . . be performed in order to facilitate transactions on the blockchain." Aleksandr Bulkin, *Explaining blockchain—how proof of work enables trustless consensus*, KEEPING STOCK (May 3, 2016), https://keepingstock.net/explaining-blockchain-how-proof-of-work-enables-trustless-consensus-2abed27f0845 [https://perma.cc/F37X-A7PQ]. For the original, albeit highly technical, discussion of proof-of-work, see Nakamoto, *supra* note 24, at 3.

50. NORTON ROSE FULBRIGHT, *supra* note 10, at 11. Such requirements include anti-money laundering provisions and proof a participant knows the client. *Id.*

51. *Id.*

52. For a visual depiction of permissioned and permissionless ledgers and their varying degrees of centralization see *id.* at 12.

53. *Id.* at 11.

54. *Id.*

cryptographic key are able to look at the individual transactions within the blockchain.[55]

The blockchain technology and the choices afforded to its users, such as permissioned, permissionless, and hybrid ledgers, are crucial to the future of smart contracts.[56] The use of blockchain allows a smart contract to be both self-verifying and fully automated. Not only do these features make potential contractual breaches more difficult, but they also make contracting with smart contracts cost effective.[57] By inputting the contractual terms into a blockchain, the nodes are able to check whether certain terms have been met. If the nodes find such terms valid, then the conditional contractual terms are triggered and the smart contract is performed.[58] Conversely, if the nodes are not able to verify the initial contractual terms, then the block is not formed and the contract is not performed.[59]

II. GENERAL ISSUES IMPEDING THE IMPLEMENTATION AND ENFORCEMENT OF SMART CONTRACTS

A. Translating Natural Language into Computer Code and Incurred Complications

As discussed earlier, the smart contract concept encompasses a variety of definitions.[60] Although flexibility can be a benefit, it has presented some issues regarding the implementation of smart contracts.[61] The spectrum of

55. *Id.*

56. Although other methods to verify a transaction exist, blockchain technology has garnered more attention and capital than the rest. Therefore, this particular technology has been dubbed "the one to work with." *See* Raskin, *supra* note 27, at 308 n.8.

57. For this reason, the use of blockchain allows a smart contract to achieve Szabo's initial goal of reducing the probability of a contractual breach by erecting barriers to protect against a potential breach.

58. Some smart contracts use oracles when determining whether certain contractual terms have been met. Typically, oracles are used in smart contract systems that are deterministic. A deterministic system relies on outside information when determining whether certain contractual terms have been met. Oracles are used in such systems as a way for the smart contracts to interact with the real world. Thus, oracles are "trusted entities which sign claims about the state of the world. Since the verification of signatures can be done deterministically, it allows deterministic smart contracts to react to the (non-deterministic) outside world." Stefan Thomas & Evan Schwartz, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, CODIUS (July 18, 2014), https://github.com/codius/codius-wiki/wiki/White-Paper [https://perma.cc/S6KW-942X]. For a potential application of oracles and smart contracts with interest rate swaps, see Cieplak & Leefatt, *supra* note 8, at 423.

59. *See* MCKINLAY ET AL., *supra* note 32, at 5 ("[A] block is only added to the chain if the nodes . . . reach consensus on the next 'valid' block to be added to the chain.").

60. *Supra* Part I.A.

61. NORTON ROSE FULBRIGHT, *supra* note 10, at 13. As addressed above, smart contracts heavily rely on technology. Many of the issues impacting widespread acceptance of smart contracts rest on the

definitions can range from one extreme, where the code itself is the contract, to another extreme, where the contract consists almost wholly of natural language. In the latter example, only smaller features, such as the payment mechanism, would be automated through the code.[62]

In addition to these rather polarizing options for smart contract implementation, there are some intermediate possibilities. These options include duplicating the translation of the smart contract into both code and natural language,[63] or a hybrid version that utilizes code to carry out the performance for non-human provisions and natural language for human performance provisions. In all the above examples, both the code and natural language aspects work together to create a unified contract.[64]

Given the above-mentioned options, the idea that a smart contract should allow the natural language to be wholly replaced with computer code poses some issues. Such an extreme leaves many unanswered questions. For one, how can it be verified that the parties to the contract are defining key contractual terms in the same manner?[65] The English language consists of many words, but computer code has a significantly smaller vocabulary.[66] Other questions include determining whether it is possible to ensure that all exceptions contained in the contract are identified by the computer coders.[67] If so, is there certainty that all the parameters, contained in the natural language, are seamlessly translated into the code?[68] Even if all the above questions are answered in the affirmative, there remains yet another unanswered question: Is it possible to make sure the code is actually executed?[69] Computer glitches are common, and delay of contract performance has the potential to cost the contracting parties lots of money.

---

immaturity of the code and/or technology itself. However, the intricacies of the code are best left to the technologists; thus, they are outside of the scope of this Note.

62. *Id.*

63. This would mean that every line of code has a corresponding natural language clause. Although duplicative, this could help create a working smart contract while allowing both parties the opportunity to review and understand the contract's actual terms. However, this suggestion runs into the same problems as a full translation of the natural language into code. For more discussion on this issue, see *infra* Part II.A.

64. NORTON ROSE FULBRIGHT, *supra* note 10, at 13. Hybrid contracts are commonly referred to as "split" contracts. *Id.*

65. CHRISTOPHER D. CLACK ET AL., SMART CONTRACT TEMPLATES: FOUNDATIONS, DESIGN LANDSCAPE AND RESEARCH DIRECTIONS 10 (Aug. 4, 2016), https://arxiv.org/pdf/1608.00771.pdf [https://perma.cc/T3J5-DZAH].

66. Raskin, *supra* note 27 at 324–25 .

67. *See* CLACK ET AL. *supra* note 65 at 11 ("Another challenge is whether such a contract, written in a computer-like language, would be admissible in court as a true and faithful representation of the intentions of the parties.").

68. *Id.*

69. *Id.*

Even though smart contracts generally offer great benefits,[70] such technological risks that arise from an attempt to fully translate a contract's natural language into computer code could limit a smart contract's economic benefits.

In an attempt to remedy some of these technological issues, advocates for smart contracts have proposed creating a standard language to help ease the process of translating natural language into code.[71] One such language is called Common Language for Augmented Contract Knowledge (CLACK).[72] Unlike traditional contracting, where the contract is read as a whole in order to interpret and hypothesize the intent of the parties, the authors of CLACK hoped this language would help reduce ambiguity by making any contractual meaning easily deducible.[73] CLACK was created to propose a simple and natural solution to the above-mentioned translation issues.[74] Instead of using traditional legal language, CLACK proposes that lawyers use the CLACK language to draft contracts.[75] In theory, CLACK would eliminate the ambiguity that may arise from nuanced word choices and social norms.[76] However, creating a standardized language to understand a different, and rather foreign language—the computer code itself—is a cumbersome solution to translating natural language into code. Yet, solutions like CLACK are one viable possibility towards advancing the use of smart contracts.

Other issues arise when the natural language of a contract is translated into computer code. For example, contract interpretation, usually done with the help of a judge, must now be done through the computer code. Typically, the process of contract interpretation involves the determination of fact-specific questions that require judgment calls and vary in degree.[77] In traditional contracting, this interpretation has been done with the help of a judge who carries the power of legal enforcement.[78] Although one of the main goals behind smart contracting is to eliminate the intermediaries, the

70. *See supra* Part I. These benefits include cost effectiveness via streamlining the contracting process by eliminating the middleman.

71. *See* CLACK ET AL., *supra* note 65, at 11 (arguing that the creation of a formal language would eliminate ambiguity and the resulting language would be simple and easy to use).

72. *See* Dr. Chris Clack, Senior Lecturer, Univ. Coll. London, Smart Legal Contracts: Prose, Parameters, Code, Presentation at the Smart Contract Templates Summit (June 29, 2016) [https://perma.cc/YJV4-4WL5]; *see also* CLACK ET AL., *supra* note 65 at 13 n.8.

73. CLACK ET AL., *supra* note 65, at 11.

74. *Id.*

75. *Id.*

76. *Id.*

77. NORTON ROSE FULBRIGHT, *supra* note 10, at 14.

78. Examples of potential questions that are commonly litigated in contract disputes and require legal judgment include whether the adverse change is material; whether best efforts were used to execute the contract; whether these efforts were reasonable; and whether there was a good faith effort. *Id.*

process of determining questions that vary in degree is difficult to complete merely through computer code.[79]

B. The Difficulties with Determining Whether and How Smart Contracts Fit Within Our Traditional Legal Notions

Another issue impeding the implementation of smart contracts relates to the fundamental notion of what constitutes a smart contract and how to best make sense of smart contracting in lieu of traditional contracting. The advent of technology has complicated not only our notion of traditional contracting but also our idea, use, and implementation of smart contracts. Such complications include the application of traditional notions of contracting to smart contracts. Despite the differences between traditional and smart contracting, it is best not to debate *whether* traditional notions apply; rather, it is more suitable to consider *how* these traditional principles apply.[80] Given what will be discussed later, it is unlikely that the mere electronic nature of smart contracts will impede their development.[81] Instead, the uncertainty and abstract form new technology can take are concepts more likely to present greater issues. Specifically, questions about what constitutes the contractual terms, along with other tangential technical requirements necessary to implement the smart contract form, are likely to pose enforceability and jurisdictional problems.

C. Reoccurring Enforcement Issues

Lastly, actual enforceability remains an issue for smart contracts. In general, contracts require enforcement in order to serve a purpose. Therefore, the goal for any form of contracting should be legal enforcement.[82] Unfortunately, smart contracts face some roadblocks in the enforcement arena. By their nature, smart contracts lack a central administrating authority. Although the lack of a centralized decision maker may have its benefits, such as cost-effectiveness, efficiency, and streamlining the contracting process, the lack of a centralized body also

79. *Id.*

80. *Id.* at 15.

81. *Id.* Later, this Note compares smart contracting to the once-contentious concept of electronic clickwrap agreements. *See infra* Part III. Clickwrap agreements are a form of electronic contracting that has become widely accepted by courts and consumers. *See id.* Like clickwrap agreements, smart contracts will become more commonplace. Because smart contracts are fundamentally similar to clickwrap agreements, the fact that smart contracts are electronic should not itself be problematic.

82. *See infra* Part VI.

means that there is no immediate authority to resolve disputes.[83] Additionally, a main tenet of blockchain technology is anonymity. Yet, if the parties' identities are unknown, then there can be no clear defendant. This makes malfeasance difficult to remedy.[84] Moreover, the contract itself can pose some enforceability issues: if the contract is the code, when did the contract become legally binding? There are two possible answers: when the contractual terms were agreed upon or when the initial contractual terms were met.[85] The aforementioned questions have no concrete answers, and this uncertainty has created some overarching issues smart contracts must face before acceptance is possible.

D. A Cautionary Tale: The DAO Hack, an Example of the Difficulties Surrounding Enforcement of Smart Contracts

Since the mid-1990s, the idea of smart contracts has created excitement and anticipation. Unfortunately, all this excitement may have rushed the implementation of a complex smart contract. With the advent of blockchain technology Decentralized Autonomous Organizations (DAOs) have become a new tool for crowdsourcing investments.[86] In June 2016, a hacker attacked a DAO, utilizing a blockchain based smart contract, and stole in excess of $70 million USD. This hacking incident[87] explores a common question: what happens when the blockchain technology works but the code and the contractual clauses are faulty?[88] When considering what it takes to

---

83. A centralized body could become helpful when determining whether code defects are a liability issue for the creator of the code or the nodes. *See* MCKINLAY ET AL., *supra* note 32, at 8–10.

84. Likewise, given the format of blockchain, this anonymity makes it difficult to disseminate and enforce a court award. *Id.*

85. *Id.* at 19–20. The referenced White Paper suggests placing a dispute resolution clause within the contract itself in order to help make the smart contract enforceable. Although this may help, other issues such as debate surrounding the true meaning of contract terms or the point at which the contract actually existed, may still persist.

86. Antonio Madeira, *The DAO, The Hack, The Soft Fork and The Hard Fork*, CRYPTOCOMPARE (July 30, 2018), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/ [https://perma.cc/BGA2-HD87]. For more information on the structure of the DAO and the hack, see Siegel, *infra* note 88.

87. *See* Klint Finley, *A $50 Million Hack Just Showed That The DAO Was All Too Human*, WIRED (June 18, 2016, 4:30 AM), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [https://perma.cc/SP6L-WTU5]; Rob Price, *Digital currency Ethereum is cratering because of a $50 million hack*, BUS. INSIDER (June 17, 2016, 5:34 AM), https://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6 [https://perma.cc/5XT6-A9LS].

88. It is important to note that the Ethereum blockchain itself was not, and has never been, hacked. Ethereum blockchain continues to support and execute many other smart contracts. Rather, the June 2016 hack was based on a recursive flaw in the smart contract's code. David Siegel, *Understanding the DAO Attack*, COINDESK (June 25, 2016, 4:00 AM), https://www.coindesk.com/understanding-dao-hack-journalists [https://perma.cc/C8WL-BW6Y].

achieve widespread use, it is important to review past errors in order to create future remedies. The 2016 hack serves as a cautionary tale for why mature and tested technologies are necessary before smart contracts can achieve widespread acceptance.

In May 2016, a DAO, called the Genesis DAO, was created with the purpose of operating a venture capital fund for cryptocurrencies.[89] Under the structure of a DAO, users invest their cryptocurrency, Ether, into a pool. In exchange, the users are able to vote on how the Ether pool is invested.[90] Theoretically, the benefits of using a DAO, which lacks any centralized authority, are two-fold: reduced costs and increased control over investments.[91]

The Genesis DAO revolved around a complex smart contract built on Ethereum blockchain. With the help of a smart contract, investors were able to send Ether and vote on possible investments.[92] Under the Genesis DAO structure, if a selected proposal reached a twenty percent quorum, then the DAO would initiate the investment on behalf of the pooled investors. However, investors were not bound to any specific investment.[93] The DAO included a special "exit door" or "split function" that could be triggered by any investor who felt an investment may damage their portfolio.[94] Thus, this exit door allowed users to leave the DAO. Once the exit door was initiated, the users would receive their remaining Ether.[95]

Although the invention of this DAO seemed promising, just two months after its inception, the advancement was forced to take one giant step back. On June 18, 2016, a hacker entered the "impenetrable" DAO through the smart contract's exit door policy.[96] A clever malfeasant user exploited a

---

89. *See* Siegel, *supra* note 88. The Genesis DAO was an immediate hit. By the end of the funding period the DAO far surpassed its creator's expectations, raising in excess of $150 million USD.

90. *Id*.

> The DAO had a creation period during which anyone was allowed to send Ether to a special wallet address in exchange for DAO tokens on a 1–100 scale. The creation period was an unforeseen success as it managed to gather 12.7 Ether (worth around $150M USD at the time), making it the biggest crowdfund ever. At some point, when Ether was trading at $20, the total Ether from the DAO was worth over $250 million.

Madeira, *supra* note 86.

91. *See* Siegel, *supra* note 88. It is important to note that under the structure of a DAO, investors only gain voting rights and not ownership of the DAO. The DAO is simply software that runs on the Ethereum network. *Id.*

92. Madeira, *supra* note 86.

93. *Id.*

94. *Id.*

95. *Id.* When an investor left the DAO, a "child DAO" was created, and the investor's remaining money would be sent to that child DAO after a twenty-eight-day waiting period. The investor would then be able to access their remaining Ether through their child DAO. *Id.*

96. *Id.* Even before the hack happened, some investors pointed out the flaws in the smart contract's code. On June 12, 2016, six days before the hack, Stephan Tual, a creator of the DAO,

flaw in the smart contract's recursive code. This flaw allowed the hacker to repeatedly request an exit. Each time an exit was requested, Ether was sent to a "child" DAO.[97] In effect, the hacker's repeated exits continually sent Ether to this child DAO before the Genesis DAO was able to register the original exit, update the total remaining Ether, and cut off the transactions.[98] In a matter of hours, the hacker drained the DAO of 3.6 million Ether. At the date of the hack, this amount was valued at approximately $70 million USD.[99]

One of the reasons why the DAO was unable to force the hacker to replace the stolen Ether stems from the purpose of Ethereum, which is a form of popular blockchain technology predominantly utilized for smart contracts.[100] Similar to other forms of blockchain technology, the Ethereum system is designed to *prevent* transactions from being undone.[101] Blockchain programing is "intrinsically unrevertible."[102] As discussed above, the goal for smart contracting is to create a contract that is irrevocable and automated.[103] When these two features are combined and the smart contract is initiated, the reality becomes an irreversible smart contract with potential code flaws for users to exploit. The DAO hack, in combination with the purpose of Ethereum and smart contracting, highlights one reason why smart contracts can create risky situations for their users.

---

announced the presence of a "recursive call bug;" however, he mistakenly believed that none of the DAO funds were at risk. Siegel, *supra* note 88.

97. Madeira, *supra* note 86.

98. *See* Haseeb Qureshi, *A hacker stole $31M of Ether—how it happened, and what it means for Ethereum*, FREECODECAMP (July 20, 2017), https://medium.freecodecamp.org/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce [https://perma.cc/DCS8-SDEC].

99. Madeira, *supra* note 86. This hack was a major setback for the DAO. Because the DAO controlled approximately fifteen percent of all Ether, any failure could negatively impact the entire Ethereum network. For these reasons, the creators of the DAO had a strong incentive to remedy the hack as soon as possible. In an attempt to remedy the situation, the creators had to quickly choose between a soft-fork and a hard-fork option for the code. Under the soft-fork option, Vitalik Buterin of the Ethereum Foundation proposed "install[ing] a 'switch' in the basic [E]thereum code that [would prevent] moving any ether out of the DAO or its children." Siegel, *supra* note 88. The hard-fork option was much more aggressive. Under the hard-fork, "the miners [would] completely unwind the theft and return all Ether to [t]he DAO, where it [could] be redeemed by token holders automatically, thereby ending [t]he DAO." *Id.* The hard-fork option was chosen. For more discussion on the public's sentiment regarding both the soft-fork and hard-fork options, see *id.*

100. *Id.* Additionally, the DAO was also unable to recognize the flaw because of the way the smart contract's code was structured. The code allowed the Ether to be removed before updating the total Ether in the DAO. Because of this structural issue, Ether was able to exit the DAO before the DAO actually registered the previous action and updated the total Ether. Qureshi, *supra* note 98.

101. Cieplak & Leefatt, *supra* note 8, at 425.

102. Qureshi, *supra* note 98.

103. *See supra* Part I.A.

In addition to the faulty recursive code, the 2016 hack also demonstrates the difficulties in achieving a suitable remedy for a smart contract hack. Ethereum is based on a permissionless public blockchain, which means parties remain anonymous.[104] Due to the anonymity of all parties involved in the Genesis DAO, there is a possibility that the identity of the hacker will never be known.[105] Initially, anonymity was considered a positive attribute of blockchain; however, this hack shows the difficulty in pursuing litigation under an anonymous system. Such a system can leave those harmed without any form of remedy. Without an identifiable defendant, it would be difficult for a plaintiff to pursue a suit for damages.[106] Thus, going against all notions of fairness and justice, the injured party remains injured.[107]

Eventually, the ending for the Genesis DAO was a bit different. The DAO investors were repaid for their loss, but it came at a great cost. The DAO was forced to make a "hard fork" split in the code. In effect, this hard fork created two Ethereum blockchains with two separate codes and incompatible cryptocurrencies.[108] Because these cryptocurrencies are incompatible, the value of Ether is now split.[109] In addition to causing a loss in Ether value, the hack and forced hard fork cost blockchain technologies and smart contracts public confidence.[110]

---

104. For more discussion on permissionless ledgers and public proof-of-work see *supra* Part I.C.

105. Although some commentators initially thought there was enough information available to uncover the hacker's identity, over two years have passed and the hacker's identity is still unknown. *See* Siegel, *supra* note 88 (stating his initial thought that others would discover the hacker's identity soon after the hack). *See also* Burgess Powell, *Ethereum (ETH) vs Ethereum Classic (ETC): What Are the Differences?*, BLOCKLR (Oct. 4, 2018), https://blocklr.com/guides/ethereum-eth-vs-ethereumclassic-etc/ [https://perma.cc/Y3TD-E4K3] (a recent reference to "an anonymous hacker").

106. *See* FED. R. CIV. P. 4(a)(1)(B) ("A summons must: be directed to the defendant"), 4(b) ("[o]n or after filing the complaint, the plaintiff may present a summons to the clerk . . . for service on the defendant.") These sections of Rule 4 prove that in order to both file and issue a proper complaint, the defendant must be identifiable. Without meeting the aforementioned requirements, cases are dismissed. *Id.* Furthermore, there is uncertainty as to whether the hacker could be held legally liable for stealing the Ether. Because the smart contract code encompassed the legal terms for the DAO investment agreement, the code itself is therefore the law. In fact, after the attack, the hacker wrote a letter to the DAO and Ethereum community claiming that the stolen Ether was his/hers. Siegel, *supra* note 88. For this reason, the hacker could potentially argue the repeated exercise of the recursive exit option was a legal possibility provided by the code. Under such rationale, the Ether was not stolen, merely legally reallocated. *Id.* For a similar concern, see Cawrey, *supra* note 5.

107. For an argument discussing the impact the lack of smart contract regulation has on plaintiffs, see *infra* Part VI.

108. Siegel, *supra* note 88.

109. The hard fork split Ethereum into two different cryptocurrencies—Ethereum and Ethereum Classic. As a result of this split, the two Ethereums are founded on different ideologies and blockchains. For further discussion on the two forms of Ethereum and how this has affected their respected values see Powell, *supra* note 105.

110. The diminished public confidence is shown through the drop in the price of Ether. As a result of the hack, the Ether price went from $20 to $13. *Id.*

The DAO hack is an example of what can happen when the code is not "exhaustively tested for every potential outcome."[111] Even though the DAO originally held great promise, the hack was a rude awakening to Szabo's hope that smart contracts will become a staple in modern society.[112] The hack has left users with diminished confidence in the current form of the technology,[113] which has effectively shattered the buzz and excitement surrounding smart contracts. As this case exemplifies, the smart contract technology is immature and not yet ready for widespread sophisticated implementation.[114]

III. A COMPARATIVE STUDY: CLICKWRAP AGREEMENTS V. SMART CONTRACTS

The introduction of smart contracts is not the first time the legal community has been faced with the question of whether or not to enforce electronic contracts. The concept of electronic contracts first surfaced with clickwrap agreements.[115]

Clickwrap agreements are agreements that "require a user to affirmatively click a box on the website acknowledging agreement to the terms of service, which are often available in a scrolling text box, before the user is allowed to proceed."[116] In reality, these agreements are rarely read by any user, yet they are legal.[117] Courts view such agreements as a necessary evil.[118] During the early stages of acceptance for clickwrap

---

111. Kasey Panetta, *Why Blockchain's Smart Contracts Aren't Ready for the Business World*, GARTNER (June 26, 2017), https://www.gartner.com/smarterwithgartner/why-blockchains-smart-contracts-arent-ready-for-the-business-world/ [https://perma.cc/AF96-Y7FZ].

112. *See* Szabo, *supra* notes 2 & 17.

113. *See* Frances Coppola, *Ethereum's DAO Hacking Shows That Coders Are Not Infallible*, FORBES (Jun 20, 2016 09:24 AM), https://www.forbes.com/sites/francescoppola/2016/06/20/the-dao-hacking-shows-that-coders-are-not-infallible/#2c236e533983 [https://perma.cc/PU2T-QXU2] (discussing the lessons learned from the DAO hack including the misplaced trust in the coders of the DAO).

114. Many people believe that in order to protect Ethereum blockchain, smart contracts must be tested and certified. *See, e.g.*, Siegel, *supra* note 88.

115. Clickwrap contracts are the technology-based predecessor of shrinkwrap contracts. According to Judge Easterbrook, "[t]he 'shrinkwrap license' gets its name from the fact that retail software packages are covered in plastic or cellophane 'shrinkwrap.'" ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996). Shrinkwrap contracts can contain licenses that "become effective as soon as the customer tears the wrapping from the package." *Id.* Although "shrinkwrap" contracts were the precursor to "clickwrap" contracts, this Note will refer to the electronic version, clickwrap agreements, as a term that encompasses both concepts.

116. Alison S. Brehm & Cathy D. Lee, *From the Chair: "Click Here to Accept the Terms of Service*," AM. BAR ASS'N (Jan. 2015) [https://perma.cc/K37Y-JLD9].

117. *See infra* text accompanying note 122.

118. Michael R. Overly, *Legal quicksand: Shrink-wrap and click-wrap agreements*, CSO (Aug. 2, 2011, 8:00 AM), https://www.csoonline.com/article/2129174/compliance/legal-quicksand--shrink-wrap-and-click-wrap-agreements.html [https://perma.cc/H9R5-D5BN]. *See also ProCD, Inc.*, 86 F.3d

agreements, public backlash revolved around the importance of clarity and fairness.[119] Often, clickwrap agreements struggled with the requirement for mutual assent: were both parties really aware of the contractual terms?[120] Despite the mutual assent concerns, it soon became apparent that without clickwrap agreements, contracting via the internet would be unenforceable. This would have put an end to the now very popular form of contracting—online shopping. Courts quickly began to reason that the terms in clickwrap agreements were no different from regular contracts. This reasoning allows courts to utilize the same traditional legal analysis when deciding whether clickwrap agreements are legally binding.[121]

Sometimes clickwrap agreements were upheld even when users acknowledged that they did not read the clickwrap contract. In these cases, the contract is still legally binding because the user clicked the "acknowledge" box. Essentially courts have found that when the user clicked the box, the user assented to the website's required notice of the contract terms.[122] Despite these seemingly unfair circumstances, the legal framework supports this version of notice and consent. For these reasons, the failure to read the terms of the clickwrap contract has not altered its enforceability.[123] Such flexibility has given clickwrap agreements the leeway to exist within a necessary, albeit narrow, space.

It is important to note that smart contracts, just like clickwrap agreements,[124] will most likely face a heightened potential for similar abuses.[125] Such abuses may include: lack of clarity in the contract's terms

at 1447, 1451–52, (Judge Easterbrook expressing his concerns that if shrinkwrap agreements were not legally allowed to govern certain situations, then our transactions would be pushed back to the "horse-and-buggy age").

119. *See* Brehm & Lee, *supra* note 116.

120. Mutual assent is considered "the manifestation by both parties of an intent to be bound." ASS'N OF CORP. COUNSEL, CONTRACTS 2.0: MAKING AND ENFORCING CONTRACTS ONLINE 6 (2012) [https://perma.cc/V7E8-WXFR].

121. Brehm & Lee, *supra* note 116. *See also* Feldman v. Google, Inc., 513 F. Supp. 2d 229, 236 (E.D. Pa. 2007) ("To determine whether a clickwrap agreement is enforceable, courts presented with the issue apply traditional principles of contract law and focus on whether the plaintiffs had reasonable notice of and manifested assent to the clickwrap agreement.").

122. Hancock v. American Telephone & Telegraph Co., 701 F.3d 1248, 1251 (10th Cir. 2012). *See also* Groff v. Am. Online, File No. C.A. No. PC 97-0331, 1998 WL 307001 (R.I. Super. Ct., May 27, 1998) (finding that although the plaintiff did not comprehend the presence of a forum selection clause, a valid contract existed because the plaintiff consented to the terms by clicking the "I agree" button); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528 (N.J. App. Div., July 2, 1999) (holding that a valid licensing agreement existed because each user was bound by Microsoft's subscriber agreement when he or she clicked "I agree" to the terms of use button).

123. Brehm & Lee, *supra* note 116.

124. For more discussion regarding the potential abuses that clickwrap agreements face, see Overly, *supra* note 118.

125. A recent example of a potential abuse coming to fruition is evident in the case Schnabel v. Trilegiant Corp., 697 F.3d 110, 126–31 (2d Cir. 2012). In *Schnabel*, website operators did not want to

and failure to provide adequate notice.[126] Because the potential for these abuses exist, it may mean that smart contracts will face initial public uncertainty. However, this is similar to the initial uncertainty surrounding clickwrap agreements. All these potential abuses are impediments towards widespread acceptance and enforceability of smart contracts. However, clickwrap agreements were able to overcome the potential for abuse by existing within a narrow area of contracting—internet transactions. In the case of smart contracts, if the risk of abuse can be lessened by enacting these contracts in a narrow category of transactions, it is likely that traditional legal standards will embrace smart contracts, just as they did with clickwrap agreements.[127]

IV. A CHANGING FRONTIER: EMERGING STATE ACCEPTANCE OF SMART CONTRACTS

Recently, regulation of blockchain technology has become a central theme surrounding the implementation of smart contracts.[128] Despite all the debate and scholarship, there are no federal regulations specifically addressing blockchain technology or smart contracts.[129] Unlike the federal government, some state governments have taken the lead in embracing

deter potential site users by forcing them to assent to a clickwrap agreement. As a result, the website decided to skip the "I accept" button, which, in effect, failed to give users the required notice and consent. *Schnabel*, 697 F.3d at 130. This case provides a helpful reminder that despite the legal system's favorable perspective regarding clickwrap agreements, courts will still invalidate such an agreement if it is considered abusive or lacks the key requirements for general contracting. *See* Richard Raysman, *Enforceability of Clickwrap Agreements Called into Question-Checklist for Best Practices in Electronic Contracting*, HOLLAND & KNIGHT (Nov. 7, 2012), https://www.hklaw.com/digitaltechblog/Enforceability-of-Clickwrap-Agreement-Called-into-Question----Checklist-for-Best-Practices-in-Electronic-Contracting-11-07-2012/ [https://perma.cc/Z3T4-GU88].

126. For a description addressing the lack of notice as a potential abuse for clickwrap agreements, see Brehm & Lee, *supra* note 116 ("The enforcement of [clickwrap] agreements turns . . . [on] whether the party had constructive notice of the terms of the agreement and thus agreed to be bound by them.").

127. For an argument that traditional contract law can be easily adapted to evaluate and enforce smart contracts, see Raskin, *supra* note 27, at 322–29. *See also supra* note 14 (discussing current projects which mimic Szabo's idea for smart property and therefore can be easily adapted to smart contracting) and *supra* note 16 (discussing additional fields that could benefit from the use of blockchain based smart contracts).

128. For more perspectives regarding regulation of blockchain-type technology, and thus smart contracts, see Carla L. Reyes, *Article: Moving beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); AARON WRIGHT & PRIMAVERA DE FILIPPI, DECENTRALIZED BLOCKCHAIN TECHNOLOGY AND THE RISE OF LEX CRYPTOGRAPHIA (Mar. 10, 2015) [https://perma.cc/8CUT-5WFN]; Primavera De Filippi & Samer Hassan, *Blockchain technology as a regulatory technology: From code is law to law is code*, FIRST MONDAY (Dec. 5, 2016) [https://perma.cc/WAF2-K5WP]; Joanna Diane Caytas, *Blockchain in the U.S. Regulatory Setting: Evidentiary Use in Vermont, Delaware, and Elsewhere*, COLUM. SCI. & TECH. L. REV. (May 30, 2017).

129. Caytas, *supra* note 128, § III(A). See *infra* Part VI covering a discussion regarding the need for and broader implications of regulating smart contracts.

smart contracts. The first trendsetters include: Arizona, Delaware, Illinois, and Nevada.[130]

A. Arizona

In March 2017, Arizona amended the Arizona Electronic Transaction Act[131] with the purpose of granting electronic form records and signatures

130. Jeffrey Neuburger, *Arizona Passes Groundbreaking Blockchain and Smart Contract Law – State Blockchain Laws on the Rise*, NEW MEDIA AND TECH. L. BLOG (Apr. 20, 2017), https://perma.cc/E8Z8-HRB5. Other states have instituted laws regarding blockchain technology. Hawaii passed a House Draft of H.B. 1481 on January 25, 2017. This bill is similar to Illinois's Blockchain initiative. *See infra* Part IV.C. H.B. 1481 was sent to Hawaii's Senate for review and awaits a vote. H.B. 1481, 29th Leg., Reg. Sess. (Haw. 2017), https://perma.cc/59ZX-LAD5 (last visited Aug. 22, 2018). Additionally, New York has passed blockchain legislation; however, this legislation is not statewide. Rather, New York was the first state to regulate via rulemaking. As a result of these rules, licenses are now required for businesses dealing in virtual currency in New York. A few bills were introduced in the New York legislature; however, they failed to pass with the requisite votes. These bills focused on using blockchain technology to protect voter records (A.B. 8792), define blockchain and recognize the validity of blockchain signatures (A.B. 8780), and create initiatives to study the benefits and promote the use of blockchain technology (A.B. 8793, A.B. 8783, A.B. 9685). A.B. 8792, 2017 Leg., Reg. Sess. (N.Y. 2017); A.B. 8780, 2017 Leg., Reg. Sess. (N.Y. 2017); A.B. 8793, 2017 Leg., Reg. Sess. (N.Y. 2017); A.B. 8783, 2017 Leg., Reg. Sess. (N.Y. 2017); A.B. 9685, 2018 Leg., Reg. Sess. (N.Y. 2018). Additionally, Nebraska is another state that has seen some movement regarding blockchain laws. Although not yet passed, Nebraska has proposed a law that would prohibit local municipalities from regulating blockchain technology (L.B. 694). L.B. 694, 105th Leg., 2nd Sess. (Neb. 2018). West Virginia is also looking to use blockchain technology in novel and creative ways. West Virginia piloted a program which allowed absentee military voters to use a mobile app, driven by blockchain technology, to cast their vote. This program was used in the November 8, 2018 statewide election. Terry Nguyen, *West Virginia to offer mobile blockchain voting app for overseas voters in November election*, WASH. POST (Aug. 10, 2018), https://www.washingtonpost.com/technology/2018/08/10/west-virginia-pilots-mobile-blockchain-voting-app-overseas-voters-november-election [https://perma.cc/93L6-9EHF]. *See also* Makena Kelly, *Nearley 150 West Virginians voted with a mobile blockchain app*, THE VERGE (Nov. 10, 2018 2:00 PM), https://www.theverge.com/2018/11/10/18080518/blockchain-voting-mobile-app-west-virginia-voatz; *West Virginia Not Planning to Expand Use of Blockchain Voting*, GOV'T TECH. (Nov. 9, 2018), http://www.govtech.com/products/West-Virginia-Not-Planning-to-Expand-Use-of-Blockchain-Voting.html.

Even though some states have embraced blockchain technology, others states, such as Florida and Maine, have failed to pass similar legislation. Florida H.B. 1357 allowed "electronic credentialing," and later blockchain applications for licensing and titling of vehicles. The Florida law would have also upheld contracts that utilized an electronic record containing a smart contract term. H.B. 1357, 2018 Leg., Reg. Sess. (Fla. 2018). Much like Florida's law, Maine S.B. 950 also failed to pass the legislature. The Maine law focused on creating a task force to study the possibilities of using blockchain technology in voting elections. S.B. 950, 128th Leg., Reg. Sess. (Me. 2017). Additionally, Vermont signed Act 51 into law; but, the state reneged on this law just one year later. Despite this failure, Vermont has embraced blockchain technology in other avenues. Vermont's Rules of Evidence, § 1913, holds that blockchain ledgers are considered "business records" under Evidence Rule 902. *See* VT. STAT. ANN. tit. 12, § 1913 (2016). Furthermore, Vermont's S.B.135 allowed for a study into the benefits of blockchain. In May 2018, Vermont's S.B. 269 took the state's blockchain laws one step further by defining "blockchain," pushing for a study into the use of blockchain for government records, allowing for the creation of blockchain-based limited liability companies, and holding that any fact found on a blockchain is considered authentic. S.B. 269, 2018 Leg., Reg. Sess. (Vt. 2018). *See also* Caytas, *supra* note 128.

131. ARIZ. REV. STAT. § 44-7003 (2017).

the same enforceability as traditional forms and signatures.[132] Essentially, this act gives legal effect to all electronic signatures on blockchain.[133] The Arizona law is broad and does not require the use of any one platform.[134] The new law's broad terms will allow the residents of Arizona to choose which blockchain platform to utilize—Ethereum, Bitcoin, etc.—while still giving the smart contracts legal effect.[135] Additionally, Arizona has made further amendments to their blockchain regulations. The Arizona legislature recently cleared a law that allows individuals to run blockchain nodes from within their homes.[136]

B. Delaware

In addition to Arizona, Delaware is another state that has embraced blockchain technology. In July 2017, Delaware became the first state to implement blockchain technology by "legally recogniz[ing] . . . records . . . stored on a blockchain."[137] In effect, this new law allows companies to "keep their list of shareholders on a blockchain."[138] These exciting pieces of legislation are just the start for Delaware.[139] After signing the bill into

---

132. Neuburger, *supra* note 130. For all states passing blockchain-friendly legislation one glaring question remains: Does the Federal E-Sign Act preempt a state's push to embrace blockchain and smart contracts? *Id.* The Federal E-Sign Act gives legal effect to electronic signatures. There is an ongoing concern that the Federal E-Sign Act preempts a state's own blockchain initiatives. When Arizon, and many other states, adopted blockchain friendly legislation, Arizona did so by amending their version of the UETA to include blockchain-based records under the definition of electronic records. Riley Svikhart, *Essay: Blockchain's Big Hurdle*, STAN. L. REV. (Nov 2017), https://www.stanfordlawreview.org/online/blockchains-big-hurdle/. For more discussion on federal legislation governing blockchain technologies, see *infra* Part V.

133. Aaron Stanley, *Only in Arizona: How Smart Contract Clarity is Winning Over Startups*, COINDESK (Sept. 19, 2017, 11:40 AM), https://www.coindesk.com/arizona-smart-contract-clarity-winning-startups [https://perma.cc/M8CT-B7YF].

134. *Id.*

135. *Id.* This article also speculates that Arizona's new law will make the state an increasingly popular place for start-up companies.

136. H.B. 2602, 53rd Leg., 2nd Reg. Sess., §§ 9-500.42, 11-269.22 (Ariz. 2018). In March 2018, Tennessee followed Arizona's lead and enacted a similar law which allows both blockchain technology and smart contracts to be used for electronic transactions. Additionally, the Tennessee law (S.B.1662) protects the data stored on a blockchain by protecting different ownership rights. S.B. 1662, 2018 Leg., Reg. Sess. (Tenn. 2018).

137. Michael del Castillo, *Delaware House Passes Historic Blockchain Regulation*, COINDESK (July 1, 2017), https://www.coindesk.com/delaware-house-passes-historic-blockchain-regulation [https://perma.cc/3PWG-Q3PU].

138. S.B. 69, 149th Gen. Assemb. (Del. 2017). *See* Jeff John Roberts, *Why Delaware Made it Easier for Businesses to Use Blockchain*, FORTUNE (Aug. 22, 2017), http://fortune.com/2017/08/22/fortune-500-blockchain-ledger-delaware/ [https://perma.cc/H6WE-WVF3].

139. Symbiont is the company responsible for supplying this blockchain technology to Delaware. "If successful, the tools will provide an efficient new way for companies to undertake anything from proxy votes to share splits. Firms will also be able to use the cryptographic features built into the

law, then-Governor Jack Markell of Delaware appointed an Ombudsperson and legal ambassador to the blockchain initiative[140] and asked the Delaware State Bar Association's Corporate Law Council to consider recognizing shares on a distributed ledger.[141] Additionally, Delaware's state government is required to use the blockchain technology for their public records.[142] Approximately sixty-six percent of Fortune 500 companies and eighty-five percent of initial public offerings are incorporated in Delaware.[143] Given these statistics, Delaware's new law has the potential to spur widespread effects.[144]

C. Illinois

In addition to Arizona and Delaware, Illinois has joined the group of states that are expanding their laws to make room for blockchain technology. Illinois started by creating a consortium of state and county agencies to make up the Illinois Blockchain Initiative.[145] The goal of this new Initiative is to "determine if this groundbreaking technology can be leveraged to create more efficient, integrated and trusted state services, while providing a welcoming environment for the Blockchain community."[146] In August 2017, the Illinois Blockchain Initiative started to test a blockchain-based system for digitalizing birth certificates. The goal for this program is to create technological tools that will allow both parents

blockchain to provide regulators or investors with secure temporary access to confidential documents on a case-by-case basis." Roberts, *supra* note 138.

140. In addition to providing an Ombudsman and ambassador, Delaware is working to make the new switch to blockchain technology straightforward. All of the records will remain easily accessible via a website; meanwhile, all of the blockchain technology will still happen on the back-end. This will not only help with the transition, but it will also keep the learning curve low, making corporations more likely to adapt this technology. *Id*.

141. Andrea Tinianow et al., *Delaware's 2017 Resolution: Make Blockchain a Reality*, COINDESK (Jan 3, 2017 15:30 UTC), https://www.coindesk.com/what-expect-delaware-blockchain-initiative-2017/ [https://perma.cc/LTZ7-2Z44].

142. Andrea Tinianow & Caitlin Long, *Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance*, HARVARD LAW SCH. FORUM ON CORP. GOVERNANCE AND FIN. REGULATION (Mar 16, 2017), https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/ [https://perma.cc/D2SG-7SSJ]. This initiative began with the Delaware Public Archives project. "The Public Archives project . . . uses smart records to automate compliance with the state's document retention and destruction laws and create a means by which the Delaware Public Archives can generate new revenue streams." Tinianow et al., *supra* note 141.

143. Tinianow et al., *supra* note 141.

144. In addition to widespread effects, this new blockchain initiative could be very advantageous for corporations incorporated in Delaware. Such benefits include: saving money in record keeping and transaction costs and faster auditing processes and due diligence procedures. Roberts, *supra* note 138.

145. *Blockchain in Illinois*, ILL. DEP'T OF INNOVATION & TECH., https://www2.illinois.gov/sites/doit/pages/BlockChainInitiative.aspx [https://perma.cc/TSX7-FV8J].

146. *Id.*

and doctors to instantly register the child's birth on a permissioned blockchain.[147] Under such a program, state officials will then be able to automatically verify a person's registration and "cryptographically sign data related to a person's name, date of birth, blood type, and other details."[148] Using this blockchain-based registration system means that the personal data will be stored on a permissioned "tamper-proof" distributed ledger that can only be accessed by those with the appropriate cryptographic key.[149] Although Illinois's pilot program is focused on digitizing and utilizing blockchain technology for the personal registration process, the tools that are developed for this program could aid the advancement of blockchain technology and smart contracting in other arenas.

D. Nevada

Nevada is yet another state that has begun to embrace blockchain technology. In June 2017, Nevada adopted a law that provides guidelines for the use of blockchain technology.[150] The purpose of this legislation is to "block[] local government entities from taxing, licensing and imposing other requirements on blockchain use."[151] This means that local governments and entities are not allowed to impose taxes or fees on parties using blockchain technology or smart contracts.[152] Furthermore, Nevada's law fully embraces electronic signatures recorded on blockchain by considering blockchain technology to be an electronic record protected under Nevada's UETA.[153] Nevada's legislation is similar to Arizona's bill; however, unlike Arizona, Nevada actually places specific restrictions on taxing and licensing that impede the use of blockchain-based technology.[154] These regulations, embraced by many Nevada-based business leaders,[155]

147. Joshua Althauser, *Illinois Government Pilots Blockchain Technology for Birth Certificate Digitization*, COINTELEGRAPH (Sept. 2, 2017), https://cointelegraph.com/news/illinois-government-pilots-blockchain-technology-for-birth-certificate-digitization [https://perma.cc/5D7G-3WXE]. *See* Michael del Castillo, *Illinois Launches Blockchain Pilot to Digitize Birth Certificates*, COINDESK (Aug. 31, 2017), https://www.coindesk.com/illinois-launches-blockchain-pilot-digitize-birth-certificates [https://perma.cc/2RGP-42TM].

148. Del Castillo, *supra* note 147.

149. *Id.*

150. Michael Scott, *Nevada Takes a Chance on Pro-Blockchain Legislation*, BITCOIN MAG. (June 13, 2017, 2:53 PM), https://bitcoinmagazine.com/articles/nevada-takes-chance-pro-blockchain-legislation/ [https://perma.cc/X5KQ-2GR9].

151. *Id.*

152. NEV. REV. STAT. § 268.0979 (2017).

153. See S.B. 398, 2017 Leg., 79th Reg. Sess. (Nev. 2017) (defining blockchain and incorporating blockchain based technology into the already existing definition of an electronic record).

154. S.B. 398, 2017 Leg. 79th Reg. Sess. §§ 4, 6 (Nev. 2017).

155. For example, Allison Clift-Jennings, founder of Filament, was pleased with Nevada's specific regulations because they "put[] the state at an advantage, in that it clearly and succinctly outlines

suggest that states are taking more of an active role toward not only embracing blockchain technology but also regulating the use of such technology.

V. UETA AND ESIGN: A BARE MINIMUM FOR FEDERAL REGULATION

With respect to blockchain acceptance, it is clear that there have been advances on the state level; however, federal law remains stagnant. In analyzing the widespread applicability of smart contracts, it is important to discuss the direction in which the country is headed.

At this moment, the applicable acts are Uniform Electronic Transactions Act (UETA)[156] and Electronic Signatures in Global National Commerce Act (ESIGN).[157] The purpose behind both the UETA and ESIGN is to provide a digital signature with the same validity and enforceability that a traditional signature enjoys.[158] It is important to note that, in ESIGN, Congress has allowed states to preempt either ESIGN with UETA or vice versa.[159] Essentially, Congress has granted states great deference to choose whether UETA or ESIGN best fits each state's individual goals. Such deference should not be ignored.[160] Because of this generous federal leeway, states

---

not so much what the state will do, but what the state will not do, when it comes to blockchain regulation." Scott, *supra* note 150. Filament is a Reno-based company that encourages the use of blockchain based technology for industrial use. *Id.*

156. UETA is a Uniform Act that was proposed by the National Conference of Commissioners on Uniform State Laws in 1999. For more information on the UETA, see *Uniform Electronic Transactions Act*, UNIF. LAW COMM'N (1999), http://uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act [https://perma.cc/6DLW-CJY5].

157. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106–229, 114 Stat. 464 (codified as amended in scattered sections of 15 U.S.C. § 96). ESIGN was passed on June 30, 2000, and is the federal law equivalent of the UETA.

158. *Id*.

159. *See* ESIGN § 120(a). *See also* Patricia Brumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws*, UNIF. LAW COMM'N, http://www.uniformlaws.org/Narrative.aspx?title=UETA%20and%20Preemption%20Article [https://perma.cc/6VU8-UW9Y] (discussing the parameters of ESIGN and UETA preemption).

160. Alan Cohn et al., *Steptoe Blockchain Blog: The Enforceability of Smart Contracts*, STEPTOE & JOHNSON LLP (May 4, 2017), https://www.steptoeblockchainblog.com/2017/05/the-enforceability-of-smart-contracts/ [https://perma.cc/56VJ-UUKN] (discussing ESIGN's preemption clause and congressional intent for a state to use either UETA or ESIGN in order to recognize and preserve the validity of an electronic signature). Although the UETA and ESIGN exist on the federal level, it is important to remember that the rare pieces of federal regulation that mention blockchain do so tangentially. *See How Congress is Impacting Blockchain and Crypto Regulation*, POLYSWARM, https://medium.com/polyswarm/how-congress-is-impacting-blockchain-and-crypto-regulation-an-overview-1db43824e903 [https://perma.cc/SQT4-AWM6] (citing congressional bills that mention blockchain or cryptocurrencies, a tangential relation, and finding that these bills are mostly for defense purposes). However, on the state level the situation is different. Certain states have chosen to regulate based on their willingness to cultivate an evolving technology-savvy community. It is evident that states remain free to regulate as they wish. The federal government has been slow to embrace the different states' regulations and tends to take a rather "hands-off" approach. *See* Congressional Blockchain

have been able to adopt laws that are friendlier toward the acceptance of blockchain-based technology.[161]

Both UETA and ESIGN treat digital signatures as the equivalent of traditional signatures. Although neither the UETA nor ESIGN contains specific mention of blockchain-based technology, the mere fact that these acts apply to digital signatures means they have the potential to also apply to blockchain-based smart contracts.[162] As discussed earlier, parties to a smart contract agree on the terms via a cryptographic key.[163] This cryptographic key is akin to a traditional signature. Each party has its own cryptographic key, thus making it virtually impossible for the contract to be forged. In addition to the cryptographic key, a party also needs intent to sign a smart contract. Some courts have found that "Thanks" plus a manual signature in an email creates a binding legal signature.[164] This finding

Caucus vision statement, CONG. BLOCKCHAIN CAUCUS, https://www.congressionalblockchaincaucus.com [https://perma.cc/YP 9A-TQPT] ("As a Caucus, we have decided on a hands-off regulatory approach, believing that this technology will best evolve the same way the internet did; on its own."). This is somewhat unusual behavior. Typically, the federal government exercises their preemptive power to regulate technologies affecting the financial sector. *See* Caytas, *supra* note 128, § III(A). Although blockchain technology can affect the financial industry, the federal government has yet to regulate it. Perhaps this lack of federal regulation suggests the following: the technology is too novel and the potential markets that blockchain technology touches and smart contracts govern are evolving at a pace too rapid to regulate. For these reasons, it is possible that the federal government is simply embracing an age-old federalism perspective. Under this perspective, the federal government allows the states to act as "laboratories" testing out different regulation models. *See* New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., conc.) ("It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."). Potentially, after viewing each state's regulation legislation, the federal government could enact procedures that apply on a national level. As society becomes more electronic and new technologies and uses for those technologies are created, like blockchain and smart contracts, this dialogue between the federal and state governments could signify an important future trend. For arguments that oppose the recent influx of state legislation on blockchain, see Mike Orcutt, *States That Are Passing Laws to Govern "Smart Contracts" Have No Idea What They're Doing,* MIT TECH. REV. (March 29, 2018), https://www.technologyreview.com/s/610718/states-that-are-passing-laws-to-govern-smart-contracts-have-no-idea-what-theyre-doing/ [https://perma.cc/MYB4-4W7D] (arguing that smart contracts and blockchain technology are so novel and unknown that the different states' legislation will only make future enforcement harder). *See also* Amy Davine Kim & Perianne Boring, *State-by-State Smart Contract Laws? If it Ain't Broke, Don't Fix It*, COINDESK (Feb. 26, 2018 9:00 AM), https://www.coindesk.com/state-state-smart-contract-laws-aint-broke-dont-fix [https://perma.cc/294W-8R42] (arguing that state legislation will create confusion; however federal laws ESIGN and UETA are the best mechanisms to regulate smart contracts and blockchain).

161. *Supra* Part IV.

162. For an example of a state amending its UETA to include blockchain records under the definition of electronic records, thus granting signatures on blockchain records the same UETA protections as other electronic signatures, see the discussion regarding Nevada S.B. 398 *supra* Part IV.D. This provides a helpful example of what could occur on the federal level.

163. *Supra* Part I.C.

164. Cohn et al., *supra* note 160. *See also* Roger Edwards, LLC v. Fiddes & Son, Ltd., 245 F. Supp. 2d 251, 261 (D. Me. 2003) (finding that emails containing a salutation constituted a signature that met ESIGN requirements found in 15 U.S.C § 7001(a)).

indicates that the courts are willing to accept a broad definition of what constitutes a signature. A broad definition creates a rather low bar for showing the existence of mutual assent in a smart contract. The UETA's rather lax signature requirement could potentially make it easier for a court to find smart contracts legally binding.[165]

Despite the lack of specific blockchain laws and regulations on the federal level,[166] it is possible for a court to interpret the federal law in a manner that embraces blockchain-based technology.

VI. THE VIABILITY OF SMART CONTRACTS IN THE LEGAL ARENA AND POSSIBLE FUTURE IMPLEMENTATION IN A CONTROLLED BUSINESS ENVIRONMENT

The invention of blockchain technology is exciting because it has opened the door to many potential uses and applications. The prime example is smart contracts, which utilizes the new blockchain technology to revolutionize traditional contracting. Of course, it is fun to imagine the world ten years into the future. Perhaps, with the help of both smart contracts and smart property,[167] making a trip to the store to purchase laundry detergent may be a thing of the past.[168] Despite all the excitement, it is important to consider whether society *should* move toward total implementation of smart contracts. Are smart contracts *really* as great as they sound? The idea of a smart contract is to cut out the middleman. Without the middleman, contracting is more efficient and cost-effective. However, does all this efficiency come at a cost? In this case, the cost would be the loss of the benefits the middleman offers.[169] A middleman has the

165. For a supporting argument, see Cohn et al., *supra* note 160.

166. It is important to note that, although the federal government has not yet begun to regulate blockchain-based smart contracts, some federal agencies, like the SEC, have recently started to discuss regulating cryptocurrencies, a digital form of currency that utilizes blockchain. The SEC Chairman, Jay Clayton, discussed the SEC's role in monitoring cryptocurrencies on February 6, 2018. *See Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC Before the S. Comm. On Banking, Hous., and Urban Affairs*, 115th Cong. (2018) (statement of Jay Clayton, Chairman, Securities and Exchange Commission), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission [https://perma.cc/G25T-CCRN]. On March 7, 2018, the SEC warned investors about "unregistered" online platforms being used to buy, sell, and trade tokens sold in recent Initial Coin Offerings ("ICOs"). *See* U.S. SEC. & EXCH. COMM'N, STATEMENT ON POTENTIALLY UNLAWFUL ONLINE PLATFORMS FOR TRADING DIGITAL ASSETS (2018) [https://perma.cc/9T49-JKRF]. Perhaps, the SEC's recent focus on regulating cryptocurrencies might soon turn the federal government's attention towards regulating blockchain.

167. *See supra* note 14.

168. *See supra* note 4. For more on the potential changes, see Szabo, *supra* note 17.

169. *See* Hans Rudolf Trüeb, *Smart Contracts*, WALDERWYSS, 704–06 (mentioning that because smart contracts offer a higher level of trust and security, many people hope that the use of a smart contract will eventually eliminate the need for a middleman), https://www.walderwyss.com/publicatio

potential to provide an advising and auditing role in any given transaction.[170] Without the middleman, this advice is lost, which could increase the probability of negative legal consequences.

Furthermore, smart contracts may inadvertently place the contracting parties at greater risk for technological glitches.[171] Unfortunately, it is not uncommon for technology to experience occasional malfunctions. Although smart contracts are deemed "impenetrable," this may only be true because the technology is so novel.[172] On a more realistic note, it is most likely only a matter of time before a hacker can do something malfeasant with blockchain-type technology. The June 2016 DAO hack[173] is an important reminder of why society should proceed with caution when implementing smart contracts. Just like society's caution when approaching clickwrap agreements, it is important to replicate similar apprehension when dealing with smart contracts. Even though clickwrap agreements eventually found success, these electronic agreements have remained acceptable in a rather limited set of scenarios.[174] For these reasons, smart contracts will most likely be utilized for specific scenarios as opposed to achieving success within all facets of life.[175]

ns/2278.pdf [https://perma.cc/PL3S-3VL9]; MCKINLAY ET AL., *supra* note 32, at 5 (discussing how the use of blockchain in smart contracts means that a typical intermediary is not necessary); Finley *supra* note 87 (suggesting that some of the issues caused by the 2016 DAO hack could have been avoided if the human element—the middleman—was not removed).

170. For example, take the interaction between a lawyer and client. In some instances the lawyer could be seen as a middleman. In a future where smart contracts are widespread, a client contracting to purchase land, or even a company, might choose to use a smart contract. If the client chose to contract via a smart contract, the need for a lawyer (i.e. the middleman in this scenario) would be eliminated. Consequently, the client foregoes the lawyer's auditing and advising role; thus, the client could potentially place themselves at a higher risk for bad business decisions and/or legal ramifications.

171. *See* GOVERNMENT TECHNOLOGY, *supra* note 130 (highlighting the security concern surrounding the use of the blockchain-based absentee voting application, Voatz, in future elections).

172. It is important to remember that the code used to create the DAO involved in the June 2016 hack was immature. Numerous experienced coders reviewed the lines and still failed to spot the error in time. In hindsight, some think the coding error was rather basic; however, no one thought to look for an error that minor. *See* Price, *supra* note 87; Finley, *supra* note 87. It follows that once the technology is used more frequently, others will learn from past mistakes and check their codes for similar errors. Over time the technology will become stronger. But minor errors and their amendments—which ultimately help strengthen the technology—may prove that smart contracts were not as initially impenetrable as once thought.

173. *Supra* Part II.D.

174. Overly, *supra* note 118.

175. *See also* WRIGHT & DE FILIPPI, *supra* note 128, at 8 (arguing that smart contract uses include financial sector and the regulation of governments and voting systems); Reggie O'Shields, *Article: Smart Contracts: Legal Agreements for the Blockchain*, 21 N.C. BANKING INST. 177, 178 (2017) (suggesting that smart contracts may have been overhyped); *Not-So-Clever Contracts*, THE ECONOMIST: SCHUMPETER (July 28, 2016), https://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted [https://perma.cc/4A76-5G5T] (arguing that rather than hypothesizing when, if, or how smart contracts will replace humans, this type of legal advancement is

Before smart contracts can be fully implemented, even if only within the narrow category of sophisticated business transactions, there needs to exist a function in which to regulate smart contracts. Currently, there are no federal laws specific to smart contracts, which means there is no formal regulation.[176] Because of this, smart contracts have fluid concepts regarding their legally enforceable parameters. As discussed previously, one of the major burdens faced by those injured in the DAO hack is anonymity and failure to identify a defendant.[177] Traditionally, when a case lacks an identifiable defendant, courts tend to shy away from both adjudicating and awarding damages.[178] Although regulation could stipulate how such circumstance might be handled in the court system, there is currently nothing of this sort. Without any enforceable legal framework governing and regulating smart contracts, society lacks a way to formulate, implement, and execute smart contracts. In the wake of a breach, the lack of legally enforceable parameters—coupled with the anonymity that blockchain offers—means the injured party is left to fend for themselves. This is an unsettling thought because it bucks the most primary notions of fairness and equality which the American justice system was designed to protect.[179] For these reasons, it is becoming evident that smart contracts require some form of regulation before widespread implementation can be achieved.[180]

Although regulation is required for widespread use, there are some drawbacks. For example, the purpose behind blockchain technology is similar to the purpose behind the advent of the internet. Both were created with an emphasis on promoting free expression and exchange of ideas.[181]

---

best situated in sophisticated organizations, such as banks); Panetta, *supra* note 111 (suggesting that the world is not ready for smart contracts to govern all avenues of daily life).

176. In addition to the lack of federal regulation regarding smart contracts, there is also minimal case law discussing the blockchain-based technology. Although several cases mention blockchain, only one case specifically mentions blockchain technology within the context of a smart contract, albeit in a footnote. *See In re* Dole Food Co. Stockholder Litig., Consolidated C.A. No. 8703-VCL, 2017 WL 624843, at *4 n.1 (Del. Ch. Feb. 15, 2017); Caytas, *supra* note 128.

177. *Supra* Part II.D.

178. *Supra* note 106.

179. *See* Larry A. DiMatteo, *The Norms of Contract: The Fairness Inquiry and the "Law of Satisfaction"—A Nonunified Theory*, 24 HOFSTRA L. REV. 349, 368–69 (1995) (explaining that contract law has come to embrace these norms of fairness and equality through the recognition of new equitable concepts, such as good faith, unconscionability, and promissory estoppel in modern contract theory).

180. For an example of the continued issues smart contracts face, see Jared Butcher, *Steptoe Blockchain Blog: My Smart Contract Just Ate $14 Million—Now What? Re-Thinking indemnification for smart contract risks*, STEPTOE & JOHNSON LLP (June 12, 2017), https://www.steptoeblockchainblog.com/2017/06/my-smart-contract-just-ate-14-million-now-what-re-thinking-indemnification-for-smart-contract-risks/ [https://perma.cc/WER7-54ZZ]. For an argument proposing regulation of blockchain, see Reyes, *supra* note 128.

181. For a similar perspective on the problems we face in regulating blockchain technology, see WRIGHT & DE FILIPPI, *supra* note 128, at 45–46.

However, if this technology is regulated, as is necessary for widespread use, this "free" exchange of ideas will be sacrificed.

Blockchain was created to be decentralized and is often used in connection with smart contracts, which are a self-regulating tool.[182] As previously discussed, the nodes are a self-checking and self-regulating mechanism. A new block may only be added once the majority of the nodes have reached a consensus.[183] Thus, this process of self-regulation mimics the same process of a democratic vote. Therefore, even the idea of regulating blockchain, in which someone outside of the nodes would have a say regarding how the blockchain operates, goes against its initial design. Why waste time regulating something that was created with the purpose of being self-regulating? As evident by the DAO hack, one suggested response is that the self-regulating aspect is not perfect. On the other hand, it could be argued that because the DAO hack was only made possible due to an immature contractual clause within the smart contract, not the blockchain, why not regulate smart contracts themselves? Similar to the response in opposition to regulating blockchain, regulating smart contracts also runs perpendicular to a key aspect of smart contracting. Smart contracts were created with the purpose of cutting out the middleman; however, this is only possible through the use of the quasi-democratic self-regulating process, as opposed to government regulating process, that blockchain offers. Both blockchain and smart contracts were initially intended to be self-regulating;[184] however, these questions suggest that government regulation of either blockchain or smart contracts requires regulation of the other. Thus, if widespread use is desired, it may be necessary for the government to regulate concepts that were meant to be self-regulating.

Future implementation seems to require the regulation of both smart contracts and blockchain. There are two specific components of a smart contract that would be best suited for regulation. First, regulation should require smart contracts to utilize a permissioned ledger. Second, regulation needs to target the mutuality component of a smart contract.

Smart contracts should be required to incorporate only the permissioned version of a blockchain ledger. As discussed previously, anonymity can

---

182. *See* Trüeb, *supra* note 169, at 705.

183. *See supra* Part I.C.

184. *See Blockchain Regulation and Smart Contracts*, GETSMARTER, https://www.getsmarter.com/presentations/uk/oxford-said/blockchain-regulation-and-smart-contracts (describing the self-executing process of blockchain and finding smart contracts to be "self-executing"). *See also*, Giovanni Perani, *Blockchain: is self-regulation sufficient?*, MEDIUM (May 2), https://medium.com/coinmonks/blockchain-is-self-regulation-sufficient-5bb68ac7e33f [https://perma.cc/8L4M-CMA7] (discussing the self-regulating nature of smart contracts and potential implications of regulation).

pose a serious issue for legal recourse.[185] The only way to ensure that both parties are known is to use a protected permissioned ledger. Under this form of regulation, any party who contracts via a smart contract would be required to receive a special cryptographic key. Therefore, only those parties to the smart contract could access the ledger. All other parties would be barred. This regulation would create both transparency and identity.[186] Although regulating the type of distributed ledger used may remove some of the options available to smart contracting parties, this regulation preserves the opportunity to seek a legal remedy in the event of a breach. Moreover, parties contracting with each other typically want to know with whom they are contracting. For this reason, it is unlikely that a regulation requiring all smart contracts to use permissioned ledgers will face strong opposition.[187]

In addition to requiring permissioned ledgers, regulation should also address the mutuality component of smart contracts. Traditional contracting makes use of the full spectrum of the English language. The situation is not so simple when smart contracts are involved. Because smart contracts use computer code, the contractual terms must be translated into the code.[188] However, because English words can encompass a variety of meanings to each contracting party, it is likely that neither party truly assents to what later becomes the translated terms of the smart contract. Without assent, mutuality between the parties never existed and the contracted terms are not enforceable. For this reason, mutuality requires regulation. Until computer coding becomes more advanced, one way to remedy the issue of mutuality is to require smart contracts to use a specific language.[189] Although this removes some of the freedom to contract, it also ensures that each party is aware of what they are contracting for. With the help of one language specially designed for smart contracting purposes, each party can be sure of the contract's terms. Thus, the smart contract achieves mutuality.[190]

185. For a discussion on the issues anonymity presents for legal enforcement, see *supra* Parts II.C, VI.

186. For an example of the issues that may occur when the identity of the contracting parties are not known, *see supra* Part II.D.

187. The Illinois legislation has instituted this type of permissioned ledger requirement when inputting birth certificate information on blockchain. *See supra* Part IV.C.

188. For a discussion regarding the input of English terms into computer code, see *supra* Part II.A.

189. CLACK is an example of a language created only for smart contracting. For more discussion regarding CLACK, see *supra* Part II.A.

190. It should be noted that one downside to utilizing a specialized language is that the terms contracted for will mainly be those circumstances that are straightforward. The essence of creating a specialized contracting language is to use simple terms that have the same meaning to each party. Therefore, this option makes it difficult to draft contracts with highly complex terms.

CONCLUSION

The acceptance and implementation of smart contracts presents many difficult paradoxes. Part I of this Note discussed the rather amorphous definition of a smart contract, the advent of blockchain and how this technology has aided the eventual creation of smart contracts. Additionally Part I further explored the specifics of blockchain technology and the different options for smart contracts, such as permissioned or permissionless ledgers. Part II examined the general issues impeding the implementation and enforcement of smart contracts. This section highlighted the DAO hack and explained how some of the concerns surrounding smart contracts came to fruition. Part III analogized the now commonly accepted internet contracts, clickwrap agreements, to the currently contested smart contracts. Further, Part III hypothesized that smart contracts will follow along the same path of acceptance that clickwrap agreements pursued. Part IV discussed a recent state legislation trend toward accepting blockchain technology and smart contracts. Part V mentioned the lack of federal regulation and proposed the interesting juxtaposition between the state and federal stances on regulation via UETA and ESIGN. Lastly, Part VI culminated in an analysis of smart contracts and what requirements need to be met in order to create widespread acceptance.

This Note concludes that it is necessary to first decide how and in what manner to utilize smart contracts. Although smart contracts have the potential to be all-encompassing, the recent DAO hack stands as a warning to proceed with caution. Today, the technology is vulnerable and immature; therefore, smart contracts should only be utilized under certain circumstances. Even if smart contracts are relegated to a narrow realm of the legal arena, regulation is required to ensure fairness and equality to all the contracting parties. Although smart contracts are new and rapidly evolving, in order to provide adequate remedies our legal system requires, the law needs to deal with the aforementioned concerns before widespread acceptance can occur.

Charlotte R. Young[*]

---

* J.D. (2019), Washington University School of Law; B.A. (2013), Knox College. Endless thanks to my partner, Avi, for helping me discover this Note topic (interestingly enough, a technology-based concept in something that was once very foreign to me), for constantly pushing me to explore ideas outside my comfort zone, and for acting as my steadfast sounding board. I would also like to thank my family for their continued support throughout this process. Finally, thank you to the *Washington University Law Review* for their contributions and thoughtful suggestions regarding this Note.