CONTRACTS *EX MACHINA*

KEVIN WERBACH† & NICOLAS CORNELL††

ABSTRACT

Smart contracts are self-executing digital transactions using decentralized cryptographic mechanisms for enforcement. They were theorized more than twenty years ago, but the recent development of Bitcoin and blockchain technologies has rekindled excitement about their potential among technologists and industry. Startup companies and major enterprises alike are now developing smart contract solutions for an array of markets, purporting to offer a digital bypass around traditional contract law. For legal scholars, smart contracts pose a significant question: Do smart contracts offer a superior solution to the problems that contract law addresses? In this article, we aim to understand both the potential and the limitations of smart contracts. We conclude that smart contracts offer novel possibilities, may significantly alter the commercial world, and will demand new legal responses. But smart contracts will not displace contract law. Understanding why not brings into focus the essential role of contract law as a remedial institution. In this way, smart contracts actually illuminate the role of contract law more than they obviate it.

TABLE OF CONTENTS

        †   Associate Professor, Legal Studies and Business Ethics Department, The Wharton School, University of Pennsylvania.
      ††   Assistant Professor, University of Michigan Law School.

INTRODUCTION

Technological advancements hold the potential to alter our very conception of the law. It is already common to suggest that technologies can operate as a kind of law, regulating the behavior of users.[1] But, thus far, traditional legal enforcement has generally remained available as a backstop. Is it possible for emerging technologies to displace the law even for enforcement, law's historically essential province? In this Article, we examine a significant contemporary example, digitally enforced "smart contracts"[2] based on the distributed cryptocurrency technology of Bitcoin[3] and the

---

1. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that "code is law"). This recognition in the legal academy of the constitutive role of technology follows a broader understanding within science and technology studies. *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012) (arguing that legal and technical rules governing flows of information are out of balance); Bruno Latour, *On Technical Mediation–Philosophy, Sociology, Genealogy*, 3 COMMON KNOWLEDGE 29 (1994) (analyzing the role of technological artifacts in modern day culture).

2. A smart contract is an agreement in digital form that is self-executing and self-enforcing. *See infra* note 24 and accompanying text. The term was coined by cryptographer Nick Szabo in the 1990s. *See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (Sept. 1, 1997), http://ojphi.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/53HK-9D6W].

3. Bitcoin is a digital currency not issued by any bank or sovereign state. Bitcoin first appeared in a paper published online in 2008 by "Satoshi Nakamoto." *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008) (unpublished manuscript), https://

blockchain that facilitates it.[4] Enthusiasts of various stripes believe that smart contracts offer the potential to displace the legal system's core function of enforcing agreements.[5]

It has traditionally been assumed that enforceable agreements—the lifeblood of the modern economic and social world—require the backing of a legal system. Nearly four centuries ago, Thomas Hobbes described the impossibility of binding agreements without the law:

> If a covenant be made, wherein neither of the parties perform presently, but trust one another; in the condition of mere nature (which is a condition of war of every man against every man,) upon any reasonable suspicion, it is void: but if there be a common power set over them both, with right and force sufficient to compel performance, it is not void. For he that performeth first, has no assurance the other will perform after, because the bonds of words are too weak to bridle men's ambition, avarice, anger, and other passions, without the fear of some coercive power . . . .

> But in a civil estate, where there a power set up to constrain those that would otherwise violate their faith . . . he which by the covenant is to perform first, is obliged so to do.[6]

Hobbes's basic idea—that binding agreements require a system to ensure that counterparties can trust one another to perform—is an

---

bitcoin.org/bitcoin.pdf [https://perma.cc/B777-M9F5]. Cryptocurrency is the more general term for currency-like tokens, like Bitcoin, that are secured through cryptography rather than traditional means.

4. A blockchain is a distributed ledger of transactions like the one created for Bitcoin. *See id.* ("We define an electronic coin as a chain of digital signatures."). Every node in a blockchain network verifiably sees the same transaction record, even though there is no master copy. Bitcoin uses this platform for a currency, with the ledger guaranteeing that the same coin cannot be spent twice. Smart contracts use blockchains to generalize the approach to any digitally expressible transaction.

5. *See* Matt Byrne, *Do Lawyers Have a Future?*, LAW. (Sept. 20, 2016), https://www.thelawyer.com/issues/online-september-2016/do-lawyers-have-a-future-2 [https://perma.cc/H2P4-BC94] ("Numerous futurists predict that smart contracts, using the developing technologies of blockchain and less strict coding languages, will result in contracts being written as immutable code on private blockchains, humming along harmoniously and self-executing and self-regulating."); Alan Cunningham, *Decentralisation, Distrust & Fear of the Body–The Worrying Rise of Crypto-Law*, SCRIPTED 237 (Dec. 2016), https://script-ed.org/wp-content/uploads/ 2016/12/13-3-cunningham.pdf [https://perma.cc/PAP2-VWVA] ("It is suggested that that the use of a blockchain . . . will guarantee the enforceability element of such transactions, without any need for . . . trust in the law as a reliable social praxis.").

6. THOMAS HOBBES, LEVIATHAN 91 (Oxford Univ. Press 1996) (1651). *See generally* Anthony T. Kronman, *Contract Law and the State of Nature*, 1 J.L. ECON. & ORG. 5 (1985) (examining the possibilities for assurance without state-imposed enforcement).

intuitive and powerful argument for the essential role of the law.[7]

Yet recent technological advances have led to speculation that smart contracts might largely, or entirely, displace the apparatus of contract law.[8] As one commentator succinctly puts this radical claim, "[s]mart contracts don't [need] a legal system to exist: they may operate without any overarching legal framework. De facto, they represent a technological alternative to the whole legal system."[9] Mainstream legal trade journals wonder whether "innovations offered by the Bitcoin 2.0 generation of technology may create a world where . . . technology renders some contract causes of action obsolete."[10] Even world leaders have taken notice, like Russian Prime Minister Dmitry Medvedev, who declared that "[s]mart [c]ontracts represent [a] new challenge to legal regulation. Systems creating such contracts live by their own rules, beyond the boundaries of law."[11] In short, smart contracts may offer the hope—or possibly the threat—of circumventing Hobbes's age-old essential role for the law.

The reaction to these new possibilities runs the gamut, from gleeful triumph to killjoy skepticism. Supporters claim smart contracts

---

7. *Cf.* Arthur Ripstein, *Private Order and Public Justice: Kant and Rawls*, 92 VA. L. REV. 1391, 1418 (2006) ("Private enforcement is not merely inconvenient: it is inconsistent with justice because it is ultimately the rule of the stronger.").

8. *See* DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 47 (2016) ("Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts."); Byrne, *supra* note 5; Cunningham, *supra* note 5, at 254; Rob Marvin, *Blockchain in 2017: The Year of Smart Contracts*, PCMAG (Dec. 12, 2016), http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts [https://perma.cc/2K96-PVVR] (quoting Jeff Garzik, Linux Board member, as saying that smart contracts will offer "adjudication-as-a-service," which will be "a hyper real-time version of the court system").

9. Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts as the Beginning of the End of Classic Contract Law* 21 (Nat'l Research Univ. Higher Sch. of Econ., Working Paper No. BRP 71/LAW/2016, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241 [https://perma.cc/HS7F-PF3W].

10. Andrew Hinkes, *Blockchains, Smart Contracts, and the Death of Specific Performance*, INSIDE COUNSEL (July 29, 2014), http://www.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci [https://perma.cc/6FSQ-TT47]; *see also* Byrne, *supra* note 5 ("Numerous futurist predict that smart contracts, using the developing technologies of blockchain and less strict coding languages will result in contracts being written as immutable code on private blockchains, humming along harmoniously and self-executing and self-regulating. All of a sudden, the disruption we have seen in other sectors is knocking at our own doors. But, we need not panic. At least, not yet.").

11. Savelyev, *supra* note 9, at 15 (citing Dmitry Medvedev, Vystupleniye Dmitriya Medvedeva na plenarnom zasedanii [Speech of Dmitry Medvedev on Plenary Session], Saint Petersburg International Legal Forum (May 18, 2016)).

will obviate the need for contract law, revolutionize business arrangements, and restructure property ownership.[12] Skeptics see the blockchain foundation as little more than a Ponzi scheme.[13] Some technologists argue that, despite their name, smart contracts have nothing to do with contracts.[14] One group conspicuously absent from the debate over smart contracts is contract law scholars.

Upon inspection, the story is complex. Smart contracts may or may not transform the world, but they provide real benefits and seem likely to enjoy significant adoption over time. They represent the mature end of the evolution of electronic agreements over several decades.[15] Firms can achieve significant cost savings and efficiency gains when using computers to automate contracting.[16] Smart contracts

---

12. *See, e.g.*, ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 2 (2016) ("Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world."); NORTON ROSE FULBRIGHT LLP, CAN SMART CONTRACTS BE LEGALLY BINDING CONTRACTS? 2 (2016), http://www.nortonrosefulbright.com/ knowledge/publications/ 144559/can-smart-contracts-be-legally-binding-contracts [https://perma. cc/SKV7-Z8P8] (quoting R3 consortium CEO David Rutter stating that "smart contracts . . . will set the scene for the next twenty years of finance"); *Not-So-Clever Contracts*, ECONOMIST (July 30, 2016), https://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted [https://perma.cc/E6WR-TKLH] ("Such 'smart contracts' are all the rage among futurist backers of the blockchain, the technology that underpins bitcoin, a digital currency.").

13. A Ponzi scheme is a form of investment fraud in which earlier investors are paid returns out of funds contributed by new investors, rather than from actual profits. *See Fast Answers: Ponzi Schemes*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 9, 2013), https://www.sec.gov/fast-answers/answersponzihtm.html [https://perma.cc/BFB6-4T8C]. Critics argue that the value of Bitcoin depends on a steady stream of new purchasers willing to buy the digital currency at higher prices, even though earlier purchasers (seeking investment returns) do not actually use it to buy anything, eventually causing a collapse. *See* Matt O'Brien, *Bitcoin Isn't the Future of Money—It's Either a Ponzi Scheme or a Pyramid Scheme*, WASH. POST: WONKBLOG (June 8, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/ [https://perma.cc/7BRH-Y7VE]; Eric Posner, *Fool's Gold*, SLATE (Apr. 11, 2013, 11:11 AM) http://www.slate.com/articles/ news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_ponzi_scheme_the_internet_curren cy_will_collapse.html [https://perma.cc/NQ8R-77ZB]; *see also* Ferdinando Ametrano, *Why 2017 Will Prove 'Blockchain' Was a Bad Idea,* COINDESK (Jan. 4, 2017), http://www.coindesk.com/ 2017-will-prove-blockchain-bad-idea [https://perma.cc/4HCX-PGX9] ("Probably some smart contract hype will clutter the debate, thanks to the smartest ones among the fools trying to outsmart even the smart contract inventor.").

14. *See, e.g.*, *Explainer: Smart Contracts*, MONAX, https://monax.io/explainers/ smart_contracts [https://perma.cc/45AT-KUEF] ("To begin with, smart contracts are neither particularly smart nor are they, strictly speaking, contracts.").

15. *See generally* Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012) (describing the development of data-oriented and computable digital contracts).

16. *See, e.g.*, JAMES SCHNEIDER ET AL., GOLDMAN SACHS, BLOCKCHAIN: PUTTING THEORY INTO PRACTICE (2016), https://www.scribd.com/doc/313839001/Profiles-in-Innovation-

could greatly extend those benefits, by taking advantage of Bitcoin and the blockchain as open platforms for secure exchange of value without mutual trust.[17] As they are adopted, or used in lieu of traditional contracting, smart contracts will force courts, legislatures, and other legal actors to confront difficult questions about the application of basic contract doctrines.

They will not, however, replace contract law. While smart contracts can meet the doctrinal requirements of contract law,[18] they serve a fundamentally different purpose. Contract law is a remedial institution. Its aim is not to ensure performance ex ante, but to adjudicate the grievances that may arise ex post.[19] Smart contracts bring this core function of contract law into sharper relief, as they eliminate the act of remediation by admitting no possibility of breach.[20] But, the needs that gave rise to contract law do not disappear. If the parties do not or cannot represent all possible outcomes of the smart contract arrangement ex ante, the results may diverge from their mutual intent. The parties' expression may also not produce legally sanctioned outcomes, as in the case of duress, unconscionability, or illegality. Promise-oriented disputes and grievances will not disappear, but their complexions will shift. In such scenarios, either the parties or the state will seek to reintroduce the machinery of contractual adjudication. Once one properly appreciates what is—and what is not—the function of contract law, it becomes evident that the reports of its death are "greatly exaggerated."[21]

May-24-2016-1https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1 [https://perma.cc/WP5P-JPZF] (identifying several ways to use blockchain-based smart contracts which could save billions of dollars per year).

17.   *See generally* Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 32 BERKELEY TECH. L.J. (forthcoming 2018) (conceptualizing the blockchain as a new architecture for trust).

18.   *See infra* Part II.A.

19.   *Cf.* RESTATEMENT (SECOND) OF CONTRACTS ch. 16, intro. note (AM. LAW INST. 1981) ("The traditional goal of the law of contract remedies has not been compulsion of the promisor to perform his promise but compensation of the promisee for the loss resulting from breach."); Nicolas Cornell, *A Complainant-Oriented Approach to Unconscionability and Contract Law*, 164 U. PA. L. REV. 1131, 1164 (2016) ("[C]ontract law provides a legal remedy to those who have complaints arising out of broken agreements. It is purely retrospective; it concerns the relations that occur once something impermissible is done.").

20.   *See* Hinkes, *supra* note 10.

21.   Though now part of popular culture, the familiar turn of phrase attributed to Mark Twain appears to be a slight misquotation. Twain's original comment was "the report of my death was an exaggeration." SHELLEY FISHER FISHKIN, LIGHTING OUT FOR THE TERRITORY: REFLECTIONS ON MARK TWAIN AND AMERICAN CULTURE 134 (1996).

The remainder of this Article unfolds as follows. In Part I, we describe the history and operation of smart contracts. In Part II, we evaluate smart contracts, which have been undertheorized so far, by asking how existing legal categories might apply to smart contracts. In Part III, we consider whether smart contracts can serve as a substitute for contract law. We answer this question in the negative, by analyzing the larger question of what contract law is for. In Part IV, we consider likely responses to the practical and doctrinal questions we raise. Surprisingly for the libertarian proponents of smart contracts, they may force the expansion of public law into the private law preserve of contracts.[22] The only way to prevent serious negative outcomes from smart contracts may be for governments to regulate them.

I. CONTRACTS GET SMART

The cryptographer Nick Szabo defined a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[23] By using "a set of promises," Szabo left open whether a smart contract was enforceable as a legal contract.[24] We consider this question below.[25] Szabo's reference to "protocols within which" parties perform is similarly coy. Smart contracts do not just specify these protocols; they actually implement them. Szabo's definition has not been universally adopted, and subsequent authors offer subtly varied descriptions of the term. For

---

22. *See, e.g.*, Aaron Wright & Primavera de Filippi, Decentralized Blockchain Technology and the Rise of *Lex Cryptographia* 4 (Mar. 12, 2015) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/RQR3-VJCZ] (suggesting that "[i]f blockchain technology becomes more widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, may lose the ability to control and shape the activities of disparate people through existing means").

23. Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, U. AMSTERDAM (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT winterschool2006/szabo.best.vwh.net/smart_contracts_2.html [https://perma.cc/YC35-2MXQ]. Max Raskin uses a simpler definition: "agreements wherein execution is automated, usually by computers." Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 306 (2017); *see also* Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK (June 4, 2016, 6:39 PM), http://www.coindesk.com/making-sense-smart-contracts [https://perma.cc/533S-JUAJ] ("Many debates about the nature of smart contracts are really just contests between competing terminology.").

24. Other authors on the topic include the word "contract" in their definitions. For example, Wright and de Filippi define smart contracts as "digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention." *See* Wright & de Filippi, *supra* note 22, at 10–11.

25. *See infra* Part II.A.

purposes of this Article, we define a smart contract as an agreement in digital form that is self-executing and self-enforcing.[26]

In this Part, we examine the history and workings of smart contracts. Smart contracts represent the fusion of two lines of technological development: electronic contracting and cryptography. Smart contracts were first theorized and named two decades ago, but significant interest in, and implementation of, smart contracts has occurred only recently. Smart contracts could represent merely the latest step the evolution of electronic agreements, or, smart contracts' use of blockchain technology could distinguish them from any of their antecedents.

A. *The Evolution of Digital Agreements*

Thanks to their speed and power, computers have taken over many forms of human interaction over the past half century. Email and instant messages substitute for letters and phone calls, accountants use spreadsheets and enterprise resource planning software rather than paper ledgers, and travelers use online ticketing systems rather than going to a travel agent—to give just a handful of examples. This automation has had major impacts on employment, the conduct of business, and social interactions. In many cases, it has raised significant legal and policy questions. The realm of contracting has not been immune.

Contractual agreements embodied in software code, and even their automatic performance, are nothing new.[27] For several decades, larger corporations have used electronic data interchange (EDI) formats to communicate digitally across supply chains.[28] The internet brought electronic commerce (e-commerce) to ordinary consumers, who accede to a digital contract every time they begin a relationship with an online service provider by clicking a button.[29] Despite its digital

---

26. In addition to execution and enforcement, smart contract–related technologies could support the full range of contractual activity, including precontractual negotiation, contract formation, and postcontractual modification. *See, e.g.*, OPENLAW, http://openlaw.io [https://perma.cc/D8EZ-D5PW] (offering tools to "[c]reate, store, and execute legal agreements that interact with blockchain-based smart contracts."). We explain the centrality of enforcement to smart contracts below at Part I.C.

27. *See* Surden, *supra* note 15, at 634.

28. EDI, which has been around since the 1970s, refers generally to automated digital communications between or within firms, much of which goes beyond the bounds of contracting language. *See* JANE K. WINN & BENJAMIN WRIGHT, LAW OF ELECTRONIC COMMERCE § 5-09 (4th ed. 2001) (describing EDI); Surden, *supra* note 15, at 639 n.30.

29. *See* Brett Frischmann & Evan Selinger, *Engineering Humans with Contracts* 8 (Benjamin

costume, this sort of electronic contract is still a written agreement—while it is electronic in *form*, its substance and execution are still dependent on humans. A user who clicks the hyperlink to read the terms of service for Facebook or Amazon.com would then see a document that spells out the contractual terms. Courts apply contract law to such agreements in the same way as to a paper document. The major doctrinal question raised here is acceptance, because most consumers barely realize the existence of, let alone read, the contractual text; that said, courts have little difficulty disposing of this objection.[30]

The step beyond an electronic contract is what Professor Harry Surden labels a "data-oriented" contract. In these contracts, "the parties have expressed one or more terms or conditions of their agreement in a manner designed to be processable by a computer system."[31] The distinction here is that the primary audience for the contract is a machine rather than a human.[32] For example, a financial option contract may grant the right to purchase a stock at a given price, and expire on a certain date. A data-oriented contract would represent that arrangement in computer code. A brokerage house could then, if the conditions are met, direct its computer system to transfer the security to the buyer's account and debit the correct sum.

The next stage in Surden's typology is a "computable" contract.[33] It gives the computer systems that implement data-oriented contracts the power "to make automated, *prima-facie* assessments about compliance or performance."[34] In the option contract example above,

---

N. Cardozo Sch. of Law, Faculty Research Paper No. 493, 2016), https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2834011 [https://perma.cc/VEE3-BU99].

30. *See* Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149 (7th Cir. 1997); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1452–53 (7th Cir. 1996). Courts have been willing to find the requisite evidence of acceptance lacking based on particular facts. *See, e.g.*, Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 35 (2d Cir. 2002).

31. Surden, *supra* note 15, at 639.

32. In fact, the term is even more limited. *See id.* at 640 ("The data-oriented label simply suggests that the parties have decided that *some* subset of key terms or conditions would benefit from being represented as computer processable data." (emphasis in original)).

33. Professor Lauren Henry Scholz applies a different typology of "algorithmic" contracts, defined as those "that contain terms that were determined by algorithm rather than a person." Lauren Henry Scholz, *Algorithmic Contracts*, 20 Stan. Tech. L. Rev. (forthcoming 2017) (manuscript at 12), https://ssrn.com/abstract=2747701 [https://perma.cc/64Z5-NNRD]. Scholz's focus is on formation. We believe the degree to which execution and enforcement are automated is the critical variable for thinking about smart contracts, with algorithmic formation raising its own set of issues.

34. *See* Surden*, supra* note 15, at 636.

the brokerage house computer system itself could evaluate whether the price and timing of a proposed purchase met the terms of the option. The requirements for a computable contract are that the semantics—the meaning of the contractual terms—can be expressed through a set of instructions or logic that a computer can process, and that any data necessary for that computation are available in digital form.[35] Giving machines the ability to determine whether a contract has been performed can dramatically reduce transaction costs.[36] Although there are significant challenges in accurately representing and interpreting contractual semantics in computer form, finance and similar fields employ computable contracts widely.[37]

The evolution from electronic, to data-oriented, to computable contracts embodies a trend toward greater machine autonomy. As computers can increasingly replace humans in negotiating, forming, performing, and enforcing contracts, contracts can increasingly operate with the speed and consistency of machines. Further, computable contracts can enable machines to contract automatically with one another, although such autonomous operation is still relatively limited.[38]

The limitation of computable contracts is that the computers involved can only make prima facie determinations about performance.[39] The legal system and other traditional mechanisms remain available to the parties if they are unsatisfied with the results of automated systems.[40] The contract is designed to be computable, but if the computation diverges from the parties' intent, as conventionally understood in contract law, they may disregard the computerized

---

35. *See id.* at 664.

36. *See id*. at 689–95.

37. *See id.* at 634.

38. *See id.* at 695.

39. *See id*. at 637 n.25.

40. Surden's article, which appeared in 2012, makes no reference to smart contracts or the blockchain. More recently, Flood and Goodenough show formally that financial contracts can be represented as finite-state machines, which are subject to computational interpretation. *See* Mark D. Flood & Oliver R. Goodenough, *Contract as Automaton: The Computational Representation of Financial Agreements passim* (Office of Fin. Research, Working Paper No. 15-04, 2015), http://ssrn.com/abstract=2538224 [https://perma.cc/9ZJF-9AT9]. However, Flood and Goodenough similarly fail to discuss the implications of implementing these formalized agreements as smart contracts. *Id.*; *see also* Cristian Prisacariu & Gerardo Schneider, *A Formal Language for Electronic Contracts*, *in* FORMAL METHODS FOR OPEN OBJECT-BASED DISTRIBUTED SYSTEMS 174–89 (Marcello M. Bonsangue & Einar Broch Johnsen eds., 2007) (proposing a formal language for writing electronic contracts).

result.[41]

In 1996, Szabo began to publish a series of articles and blog posts outlining the functions and technical requirements for what he labeled "smart contracts."[42] Szabo's starting point was that "protocols, running on public networks such as the Internet, both challenge and enable us to formalize and secure new kinds of relationships in this new environment, just as contract law, business forms, and accounting controls have long formalized and secured business relationships in the paper-based world."[43] He suggested that "[t]he contractual phases of search, negotiation, commitment, performance, and adjudication . . . can be embedded in [] hardware and software."[44] Many of those functions were already being implemented electronically at the time, or would be soon with the rise of e-commerce.[45] The visionary aspect of Szabo's concept was that hardware and software *alone* would handle the full lifecycle of contractual activity. Human action could be completely replaced in various parts of contractual exchange.

Szabo's smart contracts did not require fancy technology. His primary example was the humble vending machine.[46] The simple electronic mechanism of a vending machine performs two critical functions. First, it directly effectuates performance by taking in money and dispensing products. Second, it incorporates enough security to make the cost of breach (breaking into the machine) exceed the potential rewards.[47] For all practical purposes, the vending machine is

---

41. In some circumstances, those harmed by failures of computerized agreements may ultimately be held responsible for their mistake. *See, e.g.*, David Z. Morris, *Computer Error Costs T. Rowe Price $190 Million in Dell Buyout Settlement*, FORTUNE (June 4, 2016), http://fortune.com/2016/06/04/computer-error-t-rowe-price-dell/ [https://perma.cc/H3UZ-ZBSQ] (noting that T. Rowe Price was not entitled to settlement proceeds because a computerized system mistakenly voted its shares in favor of an acquisition that the firm publicly opposed). In such situations, however, the aggrieved party is still entitled to its day in court.

42. *See* Szabo, *supra* note 2; Szabo, *supra* note 23; Nick Szabo, *The Idea of Smart Contracts* (1997), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOT winterschool2006/szabo.best.vwh.net/smart_contracts_idea.html [https://perma.cc/XF47-62RC]; Nicholas J. Szabo, Presentation for Keynote Address at the IEEE International Workshop on Electronic Contracting: Smart Contracts (July 6, 2004), http://w-uh.com/download/ WECSmart Contracts.pdf [https://perma.cc/6HQU-EYR5]. The exact introduction date of the concept is uncertain; Szabo stated that he had been refining the idea of smart contracts since "the early 1990s." Szabo, *supra* note 2, at n.1.

43. Szabo, *supra* note 2.

44. *Id.*

45. *See* WINN & WRIGHT, *supra* note 28 (discussing EDI systems that firms have used since the 1970s to automate contractual transactions and other communications).

46. *See* Szabo, *supra* note 2.

47. *See id.*

the entire contractual environment for its transactions. It is not limited to the prima facie decisions of Surden's computable contracts, because its performance of the contract is effectively final.[48]

Szabo's vision, the full automation of forming and performing contracts, was ahead of its time. His work, and similar ideas by others, were recognized within the community of "cypherpunks" who design technical mechanisms to ensure security and privacy without reliance on governments.[49] However, these ideas remained largely isolated from the e-commerce world.[50]

B. *Bitcoin and the Blockchain*

The development that made Szabo's vision of smart contracts more than a mere curiosity was Bitcoin, a digital currency not reliant on governments, banks, or other intermediary institutions.[51] Since it appeared in a mysterious 2008 post by the pseudonymous Satoshi Nakamoto,[52] Bitcoin has provoked intense interest. Less than a decade after publication of Nakamoto's paper, Bitcoin has spawned an entire ecosystem of developers, entrepreneurs, investors, traders, and analysts, working toward a vision of technologically enabled economic and social transformation.[53] Over one hundred thousand firms, including major companies such as Microsoft, Dell Computer, Dish Network, Time Inc., and Overstock.com, accept Bitcoin-denominated transactions,[54] and the nominal value of Bitcoins in circulation

---

48. If the vending machine fails to perform the contract, such as when the product becomes stuck and is not dispensed to the customer, a remedy outside the machine may be available.

49. *See* Nathaniel Popper, *Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin*, N.Y. Times (May 15, 2015), http://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html [https://perma.cc/G4UE-QU4L]; Benjamin Wallace, *The Rise and Fall of Bitcoin*, Wired (Nov. 23, 2011, 2:52 PM), https://www.wired.com/2011/11/mf_bitcoin/ [https://perma.cc/7XAK-A8GY].

50. *See* Wright & de Filippi, *supra* note 22, at 10 ("[Blockchain] technology has breathed life into a theoretical concept [of smart contracts that Szabo] first formulated in 1997.").

51. As described below in this Section, Bitcoin is technically a specific implementation of blockchain-based cryptocurrencies, or more precisely, the currency token associated with that implementation. Smart contracts, the focus of this Article, may be implemented on the Bitcoin blockchain or other blockchains.

52. *See* Nakamoto, *supra* note 3. The identity of the person or persons who authored the paper remains unknown. *See* Popper, *supra* note 49.

53. *See generally* Nathaniel Popper, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (2015) (surveying the burgeoning Bitcoin community).

54. *See* S*tate of Bitcoin 2015: Ecosystem Grows Despite Price Decline*, CoinDesk (Jan. 7, 2015), http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline [https://perma.cc/KYV3-7S8J].

exceeded $110 billion in early November 2017.[55] Venture capitalists have funded scores of Bitcoin-based startups, investing over $1 billion so far.[56] Most of the world's largest financial services firms are exploring or implementing related technologies. Legal scholars are beginning to take notice as well.[57]

The core attribute of Bitcoin is that it allows unrelated individuals and organizations to have confidence in transactions without trusting intermediaries or a legal system.[58] A currency requires trust because buyers and sellers must believe that the tokens they exchange for assets of value will themselves have value. A one hundred dollar bill without the "full faith and credit" of the United States of America is just a piece of paper featuring a green portrait of Benjamin Franklin. Bitcoin supplies a mechanism of trust that does not require the backing of any trusted institution or government. And that same mechanism can be employed for other kinds of transactions.

To supply this mechanism, Bitcoin uses a technology called "distributed ledgers."[59] A distributed ledger allows any number of computers to keep an identical record of information, without reference to a central master copy—indeed, no master copy exists.[60] This allows Bitcoin users to be confident that the same user cannot spend the same digital coin multiple times, but that turns out to be just one of many ways to use distributed ledgers. Developers and

55. *See Market Capitalization*, BLOCKCHAIN (2017), https://blockchain.info/charts/market-cap [https://perma.cc/63GA-DENX].

56. *See* Garrick Hileman, *State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin*, COINDESK (May 11, 2016), http://www.coindesk.com/state-of-blockchain-q1-2016/ [https://perma.cc/6K7J-D5S8].

57. *See generally* Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015) (discussing "smart property" built on the foundation of smart contracts); Raskin, *supra* note 23 (evaluating smart contracts as a form of contractual self-help); Wright & de Filippi, *supra* note 22 (considering the implications of the blockchain and smart contracts as a new kind of law).

58. Pete Rizzo, *VC Fred Wilson: Block Chain Could Be Bigger Opportunity than Bitcoin,* COINDESK (May 5, 2014), http://www.coindesk.com/vc-fred-wilson-block-chain-bigger-opportunity-bitcoin [https://perma.cc/AW62-C74H]; Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled onto Something Much, Much Bigger*, BUS. INSIDER (Apr. 22, 2014), http://www.businessinsider.com/the-future-of-the-blockchain-2014-4 [https://perma.cc/9KFD-4XP2].

59. Strictly speaking, not all distributed ledgers aggregate transactions into chains of blocks. However, "the blockchain" is commonly used to describe all similar systems.

60. *See* Hal Hodson, *Bitcoin Moves Beyond Mere Money*, NEW SCIENTIST (Nov. 20, 2013), http://www.newscientist.com/article/dn24620-bitcoin-moves-beyond-mere-money.html#.VZmDmqa-uf4 [https://perma.cc/MUX8-S7M2]; *Blockchain: The Next Big Thing–Or Is It?*, ECONOMIST (May 9, 2015), http://www.economist.com/news/special-report/21650295-or-it-next-big-thing [https://perma.cc/JZ29-CTF5].

entrepreneurs are actively working on applying this technology to cloud file storage;[61] ridesharing;[62] name registration (as for the internet's Domain Name System);[63] crowdfunding;[64] device management for the Internet of Things;[65] online voting;[66] verification of ownership and time-stamping for digital documents;[67] prediction markets;[68] and even establishing the provenance of wine.[69]

There are three primary elements to the Bitcoin architecture: the ledger, the network, and consensus. These three elements combine to create a mechanism for ensuring trustworthiness without requiring trust in any particular institution or agent.[70] That means users can have confidence that a transaction on the network is legitimate, accurate, and not duplicated.

The first element, the distributed ledger of transactions, is commonly called the blockchain.[71] This database grows as it steadily incorporates new approved transactions. A Bitcoin transaction is a cryptographically signed[72] statement on the blockchain transferring

---

61. *See, e.g.*, MAIDSAFE, http://maidsafe.net [https://perma.cc/VYK3-GZ6L]; STORJ, http://storj.io/ [https://perma.cc/AT8D-68UM].

62. *See* Amanda Johnson, *La'Zooz: The Decentralized Proof-of-Movement "Uber" Unveiled*, COINTELEGRAPH (Oct. 19, 2014), http://cointelegraph.com/news/112758/lazooz-the-decentralized-proof-of-movement-uber-unveiled [https://perma.cc/8HRX-DUYP].

63. *See, e.g.*, NAMECOIN, https://namecoin.info [https://perma.cc/SE6M-AEAX].

64. *See, e.g.*, BLOCKTRUST, https://blocktrust.org [https://perma.cc/5NGX-HMWS].

65. *See* Paul Brody & Veena Pureswaran, *Device Democracy: Saving the Future of the Internet of Things*, IBM *passim* (2015), http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF [https://perma.cc/XC4G-3ZFF].

66. *See* Danny Bradbury, *How Block Chain Technology Could Usher in Digital Democracy*, COINDESK (June 16, 2014, 11:05 PM), http://www.coindesk.com/block-chain-technology-digital-democracy [https://perma.cc/X4RL-CTJM].

67. *What is Proof of Existence?*, PROOF OF EXISTENCE, http://www.proofofexistence.com/about [https://perma.cc/ZF9Q-TWUZ].

68. Jack Peterson & Joseph Krug, Augur: A Decentralized, Open-Source Platform for Prediction Markets *passim* (2015) (unpublished manuscript), https://bravenewcoin.com/assets/Whitepapers/Augur-A-Decentralized-Open-Source-Platform-for-Prediction-Markets.pdf [https://perma.cc/XV6G-GM3W].

69. *The Future of Wine Provenance Is Bitcoin*, VINFOLIO BLOG (Oct. 6, 2014), http://blog.vinfolio.com/2014/10/06/the-future-of-wine-provenance-is-bitcoin [https://perma.cc/W4BX-82P7].

70. *See generally* Werbach, *supra* note 17 (describing the "trustless trust" architecture).

71. *See* Fairfield, *supra* note 57, at 808.

72. A cryptographic signature is a secure means of verifying authenticity. It verifies that the transaction was authorized by the possessor of a private key, without actually distributing the key. With this approach, Bitcoin transactions can be quasi-anonymous. They are associated with a particular account, so it is often possible to correlate multiple transactions with the same account holder, but no identifying information about the account holder needs to be provided on the

Bitcoin tokens between two or more cryptographic private keys. These transactions are grouped together into blocks, with a new block appended approximately every ten minutes.[73] Every block contains an abbreviated reference, called a cryptographic hash, to the block before it, which keeps the blocks in the proper order. Anyone can view a Bitcoin's blockchain, and trace back transactions all the way to the original "genesis block" created by Nakamoto.[74] In theory, no one can alter an existing transaction, because every block is linked in an immutable sequence.[75]

The second element is the network. The blockchain is not stored in one central location.[76] Instead, computer nodes running the Bitcoin software connect in a peer-to-peer (P2P) network, where each maintains a complete copy of the blockchain. Every transaction is broadcast across the network to all nodes, which then add valid blocks to the blockchain on a regular basis.[77] Individual consumers do not need to operate a full node; they can use third-party wallet services to host their Bitcoins and connect to a service provider on the Bitcoin network.[78]

The final element, consensus, is perhaps the least intuitive aspect of Bitcoin,[79] but perhaps its most significant innovation. Decentralized trust systems are difficult because participants to a transaction may be untrustworthy, and without the involvement of a trusted central institution like a bank, parties face increased risk that the other will not comply with the agreement. Especially when there is a financial incentive to cheat or lie, some actors can be expected to do so. If there

blockchain. And therefore, unlike traditional financial transactions where the parties may not know identities but some intermediaries, like banks, do, the actual identity of those transacting may be effectively impossible to determine.

73. J. DAX HANSEN, JACOB FARBER & PATRICK MURCK, PERKINS COIE LLP, BITCOIN: A PRIMER 2–4, https://www.perkinscoie.com/images/content/1/4/v2/14394/Bitcoin-Primer.pdf [https://perma.cc/6AWT-Z6T2]. Some distributed ledger systems use data structures other than blockchains, but the basic approach is similar.

74. Making the ledger public enhances trust because no one can hide or lie about the status of any transaction. Permissioned blockchains, which are limited to identified users, do not necessarily offer the global visibility of Bitcoin. *See infra* notes 269–71 and accompanying text.

75. The technical meaning of immutability for a blockchain is actually somewhat complex. *See* Angela Walch, *The Path of the Blockchain Lexicon (and the Law)*, 36 REV. BANKING & FIN. L. 713, 734–45 (2017).

76. *See* NARAYANAN ET AL., *supra* note 12, at 8.

77. *See id.*, at 53; Nakamoto, *supra* note 3, at 3–4.

78. Individuals wanting complete independence from any intermediary can, however, still operate their own full node on the network.

79. *See* NARAYANAN ET AL., *supra* note 12, at 52–61.

is a realistic possibility that malicious actors on the Bitcoin network could steal currency, or spend the same Bitcoins multiple times,[80] legitimate users and firms would be reluctant to use Bitcoin.

The great innovation in Bitcoin is to flip the incentive structure, by giving network nodes a reason to follow the legitimate consensus rather than behave dishonestly.[81] Bitcoin's approach to consensus is known as mining.[82] Bitcoin nodes repeatedly attempt to solve cryptographic hashing puzzles based on the transactions in a proposed new block on the blockchain. These puzzles are on a sliding level of difficulty so that, roughly every ten minutes, a random node finds a solution.[83] The new block based on that solution is broadcast across the network.[84] Other nodes, after checking for validity, add the new block to the blockchain.[85] In the event of conflicts, they follow the longest chain, which is the one the majority of the network supports. The node that successfully proposes the new block receives a financial reward.

These rewards for mining make Bitcoin resistant to attacks. Miners have incentives to apply as much computing power as possible to confirm valid blocks, because that increases their chance of winning the block reward.[86] Malicious actors are effectively competing against the total computing power in the network. Their blocks will only be adopted if they can solve the hashing puzzle before someone else. And

---

80. This is known as a double-spend transaction, and is effectively printing money.

81. *See* NARAYANAN ET AL., *supra* note 12, at 61–68; Nakamoto, *supra* note 3, at 4.

82. The more technical term for the mining process is Proof of Work. *See* Nakamoto, *supra* note 3, at 3.

83. *See* Adam Back, *A Partial Hash Collision Based Postage Scheme*, HASHCASH (Mar. 28, 1997), http://www.hashcash.org/papers/announce.txt [https://perma.cc/DBV8-PR87] (describing a proof of work system to combat email spam). Because nodes must essentially use brute force to solve the puzzles, their probability of success is proportional to their computing power. However, which node finds a valid solution first is essentially random.

84. *See* NARAYANAN ET AL., *supra* note 12, at 53.

85. The network includes additional mechanisms to deal with situations where more than one valid block is proposed, whether due to an attack or network latency. Every block in the blockchain is cryptographically linked to the block before. Under the Bitcoin protocol, when given the choice, nodes add a block to the longest possible blockchain. Every new block added thus increases the confidence level that prior blocks represent the consensus. The common heuristic in Bitcoin is that after six subsequent blocks (approximately one hour), nodes can be sufficiently confident that a block will not be replaced. In Bitcoin, however, trust is probabilistic, not absolute. Applications requiring greater security might wait longer before accepting transactions from a block, but the trade-off is increased delay before they transfer the Bitcoins or associated assets.

86. *Cf.* Kevin Werbach, *Bitcoin Is Gamification*, MEDIUM (Aug. 5, 2014), https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22 [https://perma.cc/Q4Q8-4YGG] (explaining the significance of the motivational system to Bitcoin).

because every block is linked to the previous one, as the chain gets longer, it becomes more and more difficult to replace an earlier set of transactions.

An elegant aspect of Bitcoin's mining system is that those financial rewards take the form of Bitcoins themselves.[87] Because Bitcoin is accepted as a currency, and can also be exchanged for traditional currencies, miners find the rewards desirable. Yet, the only reason Bitcoin has those properties is the trust generated by mining. Mining is, in fact, the only way that new Bitcoins are created. The mining reward is halved approximately every four years, meaning there will ultimately be no more than approximately 21 million Bitcoins ever created.[88] As an alternative compensation mechanism, Bitcoin allows parties to specify transaction rewards, which are deducted from the value of a validated transaction.[89] The expectation is that, as the available mining rewards decrease, voluntary transaction rewards will become the predominant incentive for Bitcoin miners.[90]

The combination of the ledger, the network, and consensus replaces authorities like financial or central banks, which traditionally serve to reinforce trust between transacting parties. If, for example, Abby commits to paying Bob one Bitcoin every year as a dividend for each share of stock Bob holds in Abby's company, every distributed ledger in the network will correctly reflect that information, because it will be encoded into a block of transactions that is immutably linked into a sequence. At no point in the future can anyone manipulate the

---

87. *See* NARAYANAN ET AL., *supra* note 12, at 62; Nakamoto, *supra* note 3, at 4. The block reward as of mid-2017 is 12.5 Bitcoins, which equates to roughly $25,000 at contemporary exchange rates.

88. *See id.*, at 63. This enforced scarcity is necessary to support Bitcoin's value as a currency. If the number of Bitcoins could keep growing indefinitely, the currency would be subject to massive devaluation due to inflation. The Bitcoin protocol allows Bitcoins to be subdivided down to eight decimal places, with the smallest unit being designated as one Satoshi. So, even though the exchange rate of a Bitcoin is, as of mid-2017, over $2,000, transactions can involve tiny amounts of money, far smaller than the equivalent of one cent.

89. Nakamoto called these "transaction fees." *See* Nakamoto, *supra* note 3, at 4. We use "transaction rewards" to clarify that the sum is offered by the transacting party, and only paid to the node that successfully validates a block through the mining process. It is not a fee specified by nodes in order to process a block.

90. *See id.* In practice, transaction rewards have grown rapidly because the Bitcoin system has struggled to keep up with growth. Users need to attach significant rewards to incentivize miners to process their transactions quickly. *See* Joseph Young, *As Recommended Fees Go Past $2, Bitcoin Direly Needs a Scaling Solution*, CRYPTOCOINS NEWS (May 31, 2017), https://www.cryptocoinsnews.com/urgent-necessity-of-a-scaling-solution-recommended-bitcoin-fees-go-past-2/ [https://perma.cc/BSR9-BXX6].

ledger to change or delete the transaction. Abby and Bob both know this and do not need a bank to provide reassurance that the Bitcoin transaction is legitimate. As the recipient of the dividend payment, Bob can confidently spend that Bitcoin without concerns about its legitimacy.

C. *Blockchain-Based Smart Contracts*

As thus described, the blockchain is a general-purpose technology for trusted transactions. One important class of trusted transactions is contracts. A legally enforceable contract enables parties to coordinate their actions and trust that their commitments to each other will be fulfilled.[91] An inherent constraint on traditional contracting is that the parties must trust the state, and a variety of private intermediaries that facilitate efficient operation of the system. Legal enforcement of contracts can be cumbersome and prone to error. Just as there are reasons to use a decentralized digital currency system even though traditional currencies are successful, there are reasons to use decentralized digital contracts to solve problems that the conventional contract system cannot. The basic challenge for decentralized contracts is the same as for currencies: reliably ensuring that participants will follow the rules and accept their outputs.[92]

Szabo's original conception of smart contracts envisioned that cryptography would secure agreements, but had no mechanism to guarantee enforcement or transfer of value. Everything changed with the development of Bitcoin.[93] Bitcoin's success in decentralizing trusted financial transactions gives hope to those who advocate similar

---

91. *See, e.g.*, Anthony J. Bellia Jr., *Promises, Trust, and Contract Law*, 47 AM. J. JURIS. 25, 26 (2002) ("The incentive to rely on a promise exists only to the degree that a promise is trustworthy."). As Stewart Macauley famously showed, enforceable contracts enable coordination by structuring the relationship between contracting parties, even where threats of legal action are rare. *See* Stewart Macaulay, *Non-Contractual Relations in Business: A Preliminary Study*, 28 AM. SOC. REV. 55, 57 (1963); *cf.* Carolina Camén, Patrik Gottfridsson & Bo Rundh, *To Trust or Not To Trust?: Formal Contracts and the Building of Long-Term Relationships*, 49 MGMT. DECISION 365, 365 (2011) (studying empirically the role that formal contracts can play in cultivating trust). The theory behind smart contracts is built on this idea. *See* Szabo, *supra* note 2.

92. *See* FRANÇOIS R. VELDE, THE FED. RESERVE BANK OF CHI., BITCOIN: A PRIMER 1, 2–3 (2013) (stating that currencies "derive their value in exchange either from government fiat or from the belief that they may be accepted by someone else").

93. Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST COMPANY (Sept. 17, 2014), http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app [https://perma.cc/P7LX-9UFZ]; David Z. Morris, *Bitcoin Is Not Just Digital Currency. It's Napster for Finance*, FORTUNE (Jan. 21, 2014), http://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance [https://perma.cc/UV8E-U3X6].

decentralization of trusted contractual agreements.[94] Smart contracts may actually be a bigger idea than Bitcoin as a currency.[95] They take the static ledger and turn it into a dynamic system capable of executing the business logic of a contractual agreement.

Consider a simple insurance contract under which Abby promises farmer Bob, in return for a monthly payment, a lump sum in the event the temperature exceeds 100 degrees for more than five straight days during the term of the agreement. In a traditional contracting arrangement, the parties would likely reduce that agreement to a writing, signed to memorialize mutual intent. If the temperature exceeded the threshold for six straight days and Abby failed to pay, Bob could file suit for breach and present the contract as evidence. To implement a smart contract with the same terms, Abby and Bob would translate the provisions into software code. Each would make available sufficient funds to fulfill his or her side of the agreement. An agreed mechanism would be specified to determine performance, such as the daily high temperature for the area, as published on Weather.com. Abby and Bob would then each digitally sign the agreement with their private cryptographic key. One of them would send it as a transaction onto a blockchain, where it would be validated through the consensus process and recorded on the distributed ledger. Bob's payments would automatically be deducted each month and credited to Abby's account. Meanwhile, the smart contract would check the high temperature on Weather.com each day and store a record as needed on the blockchain. If the temperature exceeded 100 degrees for six days, the lump sum payment would be transferred from Abby's account to Bob's, and the smart contract would terminate.

The critical distinction between smart contracts and other forms of electronic agreements is enforcement. Once the computers determine that the requisite state has been achieved, they automatically perform data-oriented or computable contracts.

---

94. Nick Szabo, *Foreword* to CHAMBER OF DIG. COMMERCE, SMART CONTRACTS: 12 USE CASES FOR BUSINESS & BEYOND 3 (2016), http://www.the-blockchain.com/docs/ Smart%20 Contracts%20%2012%20Use%20Cases%20for%20Business%20and%20Beyond%20%20Cha mber%20of%20Digital%20Commerce.pdf [https://perma.cc/9ZZT-9NX8] ("Blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond.").

95. *See* Cassano, *supra* note 93. The currency aspect of Bitcoin is necessary, regardless of the application, because it provides the incentive structure for mining, at least in the ramp-up stage before transaction fees become dominant. Conceivably, Bitcoin could fail to have a significant impact on the financial system but still be the basis for the massive adoption of smart contracts.

Humans can interrupt that execution at any point.[96] But with a smart contract, complete execution of the agreement, including any transfer of value, occurs without any such opportunity to interrupt.[97] Accordingly, juridical forums are powerless to stop the execution of smart contracts—there is no room to bring an action for breach when breach is impossible. The computers in the blockchain network ensure performance, rather than any appendage of the state.[98] And, because blockchains run on a distributed network of independent nodes, with no central control point,[99] a litigant seeking to enjoin performance of a smart contract has no one to sue.[100]

---

96.   If a contract is executed on a traditional centralized computer system, the organization in control of that system can always stop execution. On a blockchain, no single entity controls the execution process. Furthermore, the output of a data-oriented or computable contract is at best only of provisional legal value. *See* Surden, *supra* note 15, at 637 n.25 ("[A]utomated assessments will often be 'first cut' approximations of an ultimate, legally authoritative determination as to compliance.").

97.   *See infra* Part II.B.3. The only exception to immutable execution of a smart contract is a fork which splits the entire blockchain into incompatible tracks. If enough network nodes follow the track without the smart contract, it effectively no longer exists. However, such a move is so technically and politically costly that it rarely if ever occurs on functioning blockchains. *See infra* note 177 and accompanying text.

98.   *See* Karen E.C. Levy, *Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law,* 3 ENGAGING SCI., TECH. & SOC'Y. 1, 2 (2017) ("Because they are based on code, smart contracts can be *immediately and automatically* effectuated, without . . . the intervention of institutions like courts."). The power of the smart contract is, however, limited to those assets which can be incorporated or controlled by a blockchain. A smart contract for construction of a house could not force the builder to perform, for example, nor could a smart contract to purchase a painting physically move it to the buyer's home. With techniques such as "smart property," however, more assets will be susceptible to blockchain control. *See* Fairfield, *supra* note 57, at 825–28.

99.   The organizations developing the blockchain's software have no power over the network nodes that validate transactions. Even if a court ordered the software developers to issue an update that halted a particular smart contract, the miners would not have to adopt it. And because anyone around the world can set up a mining node on a public blockchain such as Bitcoin or Ethereum, there would be no way for that court to enforce compliance by the miners.

Exactly how powerless a court would be depends on the system. It is possible to use the basic technical approach of a blockchain to execute smart contracts on a "permissioned" network in which nodes must be authenticated and approved. *See* Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems*, GREAT WALL OF NUMBERS (Apr. 6, 2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf [https://perma.cc/V36W-EFPA]. Those nodes could be contractually bound to follow duly issued judicial decisions. Even in that scenario, the practicalities of judicial oversight of the contract could be quite challenging. Further, it is unclear why a permissioned blockchain network would deliberately compromise the automation and certainty upon which the efficiency gains of smart contracts are premised.

100.   Operators of sites connected to a blockchain, such as the infamous Silk Road online marketplace for illegal transactions using Bitcoin, may be brought to the bar. Silk Road operator Ross Ulbricht was eventually caught by U.S. law enforcement authorities and sentenced to life in

The blockchain's distributed trust facilitates smart contracts between unknown or untrusted counterparties.[101] This radical decentralization is what potentially makes smart contracting a substitute for the state-based legal system, rather than an additional step before reaching that system. For example, a financial trading program that automatically buys certain stocks when prices match a predefined algorithm, could be described as a smart contract. If a dispute arises, however, the parties to that self-executing transaction will still turn to the courts, which will apply traditional legal doctrines to evaluate the agreement, ascertain breach, and impose a remedy if appropriate. With smart contracts, the transaction is irreversibly encoded on a distributed blockchain. A judicial decision holding a smart contract unenforceable cannot undo the results of its fully executed agreement.

Smart contracts are possible with Bitcoin because its protocols include a scripting language that can incorporate limited programmable logic into transactions.[102] The vast majority of transactions on the Bitcoin blockchain are simple transfers of Bitcoins between accounts.[103] Additionally, when computers on the Bitcoin network process those transfers, they can perform other functions.[104] This allows for more complicated arrangements, like delaying payment until a specified number of parties provide confirmation.

Bitcoin's native scripting language is limited. Companies are developing more powerful systems that execute the contractual logic on application servers outside the blockchain, or through alternate blockchains supporting more sophisticated scripts. The most heralded is Ethereum, a general-purpose computing platform on a blockchain foundation.[105] Ethereum is a competing system to Bitcoin. It uses the

---

prison. Kevin McCoy, *Silk Road Mastermind Ross Ulbricht Loses Legal Appeal*, USA TODAY (May 31, 2017, 11:30 AM), https://www.usatoday.com/story/money/2017/05/31/silk-road-mastermind-ross-ulbricht-loses-legal-appeal/102343062 [https://perma.cc/V56Q-SKGS]. The blockchains themselves are another story.

101. *See generally* Werbach, *supra* note 17 (describing the blockchain's "trustless trust" architecture).

102. *See* NARAYANAN ET AL., *supra* note 12, at 79–84.

103. *See id.* at 82–83 (observing that 99.9 percent of Bitcoin transactions at the time were straight transfers of coins).

104. *See id.* at 84.

105. *See* Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That Could Power the Internet of Things*, FAST COMPANY (May 21, 2015), http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could-power-the-internet-of-things [https://perma.cc/77R6-ZE3F]; *A Next-Generation Smart Contract and Decentralized Application Platform*,

same basic approach of a distributed ledger, a network of validation nodes, and consensus through mining. However, the virtual currency in the system, called Ether, is designed for purchasing computing power on the Ethereum network, rather than as an alternative to traditional currencies. Ethereum's scripting language is significantly more powerful than Bitcoin's. It is Turing complete, which means it can in theory execute any function that can be processed by a computer.[106]

The promise of Ethereum is almost comically broad: one article suggested it might "transform law, finance, and civil society."[107] While such enthusiasm may be excessive, Ethereum has gained a substantial and passionate following among developers and cryptocurrency enthusiasts. Roughly a year after Ethereum launched, there were already over three hundred distributed apps built on the platform.[108] In one of the largest crowdfunding campaigns to that point, Ethereum raised over $18 million worth of Bitcoin in the initial sale of Ether.[109] A number of more specialized blockchain-based platforms employing smart contracts launched after Ethereum.

The scripting language on a blockchain platform like Bitcoin or Ethereum can be used to determine whether the conditions for performance of a smart contract have been met, and then execute the contractual transaction without human interference.[110] In the simplest case, parties place Bitcoins or other digital currency into a suspended state on the blockchain, and once certain terms are met, those Bitcoins are transferred to the appropriate account.[111] The Bitcoins may

GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper [https://perma.cc/4DLU-SJD3]; Jim Epstein, *Here Comes Ethereum, an Information Technology Dreamed Up by a Wunderkind 19-Year-Old That Could One Day Transform Law, Finance, and Civil Society*, REASON.COM (Mar. 19, 2015), http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn [https://perma.cc/X6QU-SK83]; D.J. Pangburn, *The Humans Who Dream of Companies That Won't Need Us*, FAST COMPANY (June 19, 2015), http://www.fastcompany.com/ 3047462/the-humans-who-dream-of-companies-that-wont-need-them [https://perma.cc/MW9R-CURA].

　　106.　*See A Next-Generation Smart Contract and Decentralized Application Platform*, *supra* note 105.

　　107.　Epstein, *supra* note 105.

　　108.　*See* STATE OF THE DAPPS, http://dapps.ethercasts.com [https://perma.cc/4T99-URGE].

　　109.　Nathan Schneider, *After the Bitcoin Gold Rush*, NEW REPUBLIC (Feb. 24, 2015), http://www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle [https://perma.cc/Z7UQ-ZCUZ]. Even though Ether is not intended as a replacement for cash, it can be exchanged for other currencies at a floating rate. Demand for Ether, based on the utility of the Ethereum smart contract platform, makes the tokens more valuable.

　　110.　*See* NARAYANAN, *supra* note 12, at 286–88.

　　111.　*See* Cassano, *supra* note 93. Not all smart contracts require funds to be placed in this escrow state. First, many contracts do not involve direct transfers of funds. Second,

represent payment directly, or they may be used as tokens, associated with digital rights in assets.

This algorithmic enforcement allows contracts to be executed as quickly and cheaply as other computer code. Cost savings occur at every stage, from negotiation to enforcement, especially in replacing judicial enforcement with automated mechanisms.[112] If smart contracts are substantially cheaper and more efficient, more situations can benefit from the use of contractual agreements; for example, dynamic transactions around physical objects (smart property)[113] or offerings for those unable to afford traditional legal services.[114] Another broad attraction of smart contracts is their fundamentally decentralized nature. Those who wish to avoid trust in centralized private or governmental actors, for political reasons or otherwise, can do so and still benefit from the advantages of contract.

Even though blockchain transactions are irrevocable, there are ways to build in more flexibility. There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer.[115] It is, however, possible to incorporate logic into a smart contract that permits exceptions or conditions.[116] Enforcement could theoretically be structured to permit arbitration.[117] Such flexibility, however, must be coded into the smart contract at the outset, which takes away from the decentralization and efficiency that make smart contracts attractive

---

cryptocurrency can be used as a token to designate other assets or rights, such as title to real property. Smart contract system developers are now working through the issues involved to apply smart contracts to more complex instruments such as financial derivatives, where counterparties typically do not prefund all transactions so as to maximize liquidity. *See* Luke Clancy, *Barclays Taps Blockchain for Equity Swaps, Options, Swaptions*, RISK.NET (May 16, 2016), http:// www. risk.net/derivatives/2457777/barclays-taps-blockchain-equity-swaps-options-swaptions [https:// perma.cc/VX56-JGYK].

112.   Of course, there is a trade-off for the certainty of algorithmic enforcement, as will be discussed in *infra* Part IV.

113.   *See* Fairfield, *supra* note 57, at 825–28; Cassano, *supra* note 93.

114.   *See* Cassano, *supra* note 93.

115.   *See* Paul Vigna, *Ethereum Gets Its Hard Fork, and the 'Truth' Gets Tested*, WALL. ST. J.: MONEYBEAT BLOG (July 20, 2016 10:56 AM), http://blogs.wsj.com/moneybeat/2016/ 07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested/ [https://perma.cc/8PXE-RBRG] (describing such a "hard fork" needed to unwind a fraudulent transaction on the Ethereum network).

116.   These are simply additional terms of the contract conveyed through the scripting language of the blockchain system.

117.   Pamela Morgan, *At Bitcoin South: Innovating Legal Systems Through Blockchain Technology*, BRAVE NEW COIN (Dec. 17, 2014), http://bravenewcoin.com/news/pamela-morgan-at-bitcoin-south-innovating-legal-systems-through-blockchain-technology [https://perma.cc/ 8446-WHPN].

to begin with.

Sometimes a smart contract refers to facts in the world, for example, when a contract pays out if a stock exceeds a certain price on a certain date. The Bitcoin blockchain knows nothing about stock prices; it must collect that information through an external data feed. In the language of smart contracts, systems that interpret such external feeds and verify contractual performance are called "oracles."[118] Unlike the blockchain itself, oracles are not fully decentralized. The contracting parties must, to some degree, trust the operator of the oracle and the authenticity of its data feed.[119]

Using these capabilities, a wide variety of industries could employ smart contracts. Beyond simple financial arrangements, smart contracts could facilitate complex instruments like wills[120] or crowdfunding systems, both of which disburse funds only if certain contingencies trigger a payout.[121] Another category is smart property, for which the rights associated with objects attach to the objects themselves.[122] Networked door locks on a shared car system such as Zipcar could automatically open, but only for the individual that paid the access fee. Or, a lessor could shut off a delinquent lessee's access to a leased car, and give access to the bank, but only until full payment of

---

118. *See Smart Oracles: A Simple, Powerful Approach to Smart Contracts*, GITHUB (July 17, 2014), https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts [https://perma.cc/YWJ3-CQPQ].

119. There are, however, efforts to create distributed oracles using blockchain-based prediction markets such as Augur and Gnosis, which use financial incentives and the wisdom of crowds to evaluate statements. *See* Cade Metz, *Forget Bitcoin. The Blockchain Could Reveal What's True Today and Tomorrow*, WIRED (Mar. 22, 2017, 9:15 AM), https://www.wired.com/2017/03/forget-bitcoin-blockchain-reveal-whats-true-today-tomorrow [https://perma.cc/828D-3R58].

120. *See* Morris, *supra* note 93. A will implemented through smart contracts would specify the distribution of assets in the estate according to a set of rules. The contract could be activated with presentation of a specified private key by the executor of the estate. A hypothetical set of rules might transfer the entire balance of the estate to the private key associated with the decedent's spouse. In the event the spouse was also deceased (as verified by the executor's presentation of another private key), the funds would be divided equally among the decedent's two children. This scenario would work most simply for assets held in the form of cryptocurrencies. However, the blockchain could also record access rights to bank accounts, title to real estate, or other tokens associated with traditional assets.

121. *See* Stan Higgins, *Bitcoin-Powered Crowdfunding App Lighthouse Has Launched*, COINDESK (Jan. 20, 2015), http://www.coindesk.com/bitcoin-powered-crowdfunding-app-lighthouse-launches-open-beta/ [https://perma.cc/W7WQ-9VLN]; Paul Vigna & Michael J. Casey, *The Car of the Future May Ownerless as well as Driverless*, MARKETWATCH (Mar. 3, 2015), http://www.marketwatch.com/story/how-bitcoin-technology-could-power-driverless-cars-2015-03-03 [https://perma.cc/37NV-W5EL].

122. *See* Fairfield, *supra* note 57, at 863.

the principal. More broadly, over twenty-five billion devices comprising the Internet of Things, from light switches to crop moisture monitors, are expected to connect to the internet by 2020.[123] Smart contracts would allow these devices to operate autonomously, share resources, and exchange data without central management.[124]

Some blockchain advocates go further. They envision smart contracts as the foundation of a new kind of economic entity, the distributed autonomous organization (DAO).[125] If a corporation is simply a nexus of contracts,[126] why not encode those agreements into digital self-enforcing agreements? A DAO could have stock ownership, corporate governance rules, payroll arrangements, and virtually all of the economic trappings of a modern corporation, all running automatically in a completely distributed manner.

With the success of Ethereum and other blockchain-based platforms offering smart contracting capabilities, Szabo's twenty-year-old hypothetical has become an operational reality. Over one hundred major corporations including JPMorgan Chase, IBM, BP, Microsoft, Toyota, and Merck, have joined a consortium to promote enterprise adoption of Ethereum.[127] Many others are supporting competing initiatives.[128]

As is so often the case, though, this technology's adoption is preceding full consideration of its legal implications. Smart contracts are not just an interesting computer science innovation, because they

---

123.   *See* Colin Barker, *Is Blockchain the Key to the Internet of Things? IBM and Samsung Think It Might Just Be*, ZDNET (Jan. 21, 2015), http://www.zdnet.com/article/is-blockchain-the-key-to-the-internet-of-things-ibm-and-samsung-think-it-might-just-be/ [https://perma.cc/SR5T-ERN4].

124.   *See id.*

125.   Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAG. (Sept. 19, 2013), https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i [https://perma.cc/V8ZY-NK2J]; David Johnston et al., *The General Theory of Decentralized Applications, Dapps*, GITHUB, https://github.com/David JohnstonCEO/DecentralizedApplications [https://perma.cc/4C9S-J3ZH].

126.   Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 311 (1976).

127.   *See* Matthew Leising, *Toyota, Merck Join Ethereum Group To Build Blockchain Network*, BLOOMBERG (May 22, 2017, 12:00 AM), https://www.bloomberg.com/news/ articles/ 2017-05-22/toyota-merck-join-ethereum-group-to-build-blockchain-network [https://perma.cc/ GJ67-ZHKW].

128.   *See, e.g.*, Arjun Kharpal, *Intel and Major Banks, Including HSBC and BOAML, Pour $107 Million Into Blockchain Group*, CNBC (May 23, 2017, 8:30 AM), http://www.cnbc.com/ 2017/05/23/r3-funding-blockchain-intel-bank-of-america-hsbc.html [https://perma.cc/SV2Y-GX54] (detailing new funding for the financial industry blockchain platform R3).

tread on one of the most fundamental territories of the common law: the domain of contract.

II. CONCEPTUALIZING SMART CONTRACTS

A. *Are Smart Contracts Contracts?*

The first important question that smart contracts pose is: Are they actually contracts? Ultimately, we think the answer is "yes." But this question turns out to be ambiguous, requiring the answer to another question first: What do we mean by a "contract"? Different ways of defining contracts, in terms of legal enforceability, intent of the parties, or an exchange of promises, all complicate the analysis of whether smart contracts are contracts at all. After considering such standard definitions, we will suggest that smart contracts should nonetheless be considered contracts because they are agent-generated mechanisms to shift rights and obligations.

According to the standard legal definition, a contract is a promise or an agreement that is legally enforceable.[129] This definition, though widely accepted, has the unfortunate linguistic consequence of implying that agreements that turn out to be unenforceable were not contracts to begin with. Terms like "unconscionable contract," "fraudulent contract," and "illegal contract," all become something like oxymorons.[130] Even commonplace judicial iterations of this standard, like "[t]o be legally enforceable, a contract must be supported by consideration,"[131] become essentially redundant.

But we care about whether smart contracts are contracts in the ordinary sense, whether they are enforceable or not.[132] At a general conceptual level, are smart contracts actually contracts? So it seems

---

129. *E.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 1981) ("A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty.").

130. *But cf., e.g.*, United States v. Nunez, 673 F.3d 661, 664 (7th Cir. 2012) ("'[C]onspiracy' . . . is simply a pejorative term for a contract, both 'conspiracy' and 'contract' signifying an agreement, a meeting of minds.").

131. *See, e.g.*, Hartbarger v. Frank Paxton Co., 857 P.2d 776, 780 (N.M. 1993) ("[T]o be legally enforceable, a contract must be factually supported by an offer, an acceptance, consideration, and mutual assent.").

132. Along these lines, Thomas Joo distinguished between "Rs," which are simply relationships of reciprocal expectations and behavior, and "Ks," which are legally enforceable. *See* Thomas W. Joo, *Contract, Property, and the Role of Metaphor in Corporations Law*, 35 U.C. DAVIS L. REV. 779, 790 (2002). One way to pose the question that we are now asking would be: Are smart contracts Rs, whether or not they are Ks?

that we need a different definition of "contract" for these purposes.

One way to understand the question would be: Do smart contracts constitute promises or agreements that are *intended* to be legally enforceable? Corresponding to this formation of the question, another definition of a contract is an agreement intended to be legally enforceable, whether it turns out to be or not.[133] This definition has the advantage of avoiding the issues raised above, because it leaves open the question of enforceability. The unenforceable contract is still, conceptually, a contract as long as the parties thought that it would be enforceable, wrong though they may have been.

Of course, the intent that matters here is objective, not subjective, intent as it is manifested by the actions of the parties. As Judge Hand famously explained, "[a] contract has, strictly speaking, nothing to do with the personal, or individual, intent of the parties. A contract is an obligation attached by the mere force of law to certain acts of the parties, usually words, which ordinarily accompany and represent a known intent."[134] Still, according to this understanding, a contract exists if and only if the actions of the parties, judged objectively, manifest an intention that an agreement is to be legally enforceable.

When applied to smart contracts, this definition raises a serious issue. Smart contracts are designed to eliminate the need for legal enforcement. The central feature of a smart contract—what supposedly makes them smart—is that legal enforcement will not be necessary, or even possible. In a very real way, smart contracts are *not* intended to be legally enforceable. This is not to suggest that they are intended to be legally invalid; rather, the question of legal enforcement should never arise. In this sense, smart contracts are *not* intended to be enforced in a legal proceeding. This lack of intent may lead to the conclusion that, even conceptually, smart contracts are not truly contracts at all. They may look more like so-called "gentlemen's agreements," intended to be carried out, but never intended to reach a

---

133.   *See, e.g.*, EARL OF HALSBURY, 7 LAWS OF ENGLAND § 682 (1909) ("A contract is an agreement made between two or more persons which is intended to be enforceable at law . . . ."); *see also* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1108 (9th Cir. 2009) ("[O]nce a court concludes a promise is legally enforceable according to contract law, it has implicitly concluded that the promisor has manifestly intended that the court enforce his promise.").

134.   Hotchkiss v. Nat'l City Bank, 200 F. 287, 293 (S.D.N.Y. 1911); *see also* Lucy v. Zehmer, 84 S.E.2d 516, 522 (Va. 1954) ("If his words and acts, judged by a reasonable standard, manifest an intention to agree, it is immaterial what may be the real but unexpressed state of his mind."); RESTATEMENT (SECOND) OF CONTRACTS § 17 cmt. c (AM. LAW INST. 1981) ("[I]t is clear that a mental reservation of a party to a bargain does not impair the obligation he purports to undertake.").

courtroom.

This appearance would be misleading, however, because it is quite different to intend that a solution will not be needed than to intend that it will be unavailable. I do not intend that my car will be needed as a vehicle for escaping the zombie apocalypse, but if the zombie apocalypse comes, I do not intend to abandon my car and traverse the wasteland on foot. By the same token, smart contracts are not intended to be enforced by a court, but that's not to say that, if they end up in court, the parties intend them to be unenforceable.

It is better to think of a contract as any agreement that is meant to have practical consequences on the rights and duties of the parties—that is, is not merely aspirational.[135] This avoids the above difficulty, because whether legal enforcement was anticipated is irrelevant.[136] Smart contracts would be contracts as long as they manifest an exchange of concrete obligations. They would be contracts as long as they are meant to alter concretely the normative relation between the parties.

Yet there is still some difficulty with this definition, because this understanding of a contract requires an exchange of promises or obligations. Do smart contracts involve promises or obligations? In a significant sense, "no." The smart contract sets in motion machinery that the parties cannot subsequently prevent. The smart contract is not fulfilled by some further action of a contracting party, but rather by the completion of this mechanical process. As an analogy, if Bob balances a pail of water on top of a door, he does not promise to drop water on whoever next opens the door. Rather, he has merely set up the mechanical process by which that will inevitably happen. In a similar way, a smart contract to transfer one Bitcoin upon such-and-such event occurring is not really a promise at all. A smart contract would not say, "I will pay you one Bitcoin if such-and-such happens," but rather something like, "you will be paid one Bitcoin if such-and-such happens."

---

135. *See, e.g.*, W. David Rankin, *Concerning an Expectancy Based Remedial Theory of Promissory Estoppel*, 69 U. TORONTO FAC. L. REV. 116, 142 (2011) ("[A] contract creates rights and duties because, as purposive beings, self-determining agents may transfer the power to direct their choices to other persons, and rights and duties are required to mark the resultant scope of the parties' freedom after the transfer.").

136. *See* Gregory Klass, *Intent to Contract*, 95 VA. L. REV. 1437, 1460 (2009) (arguing that departure from any intention to create legal enforceability makes sense because "[c]ontracts create legal rights and duties" and "[t]he conditions of contractual validity function . . . to inform people of their rights and duties ex ante").

Some of the computer scientists working on smart contracts appear to be vaguely aware of this point. For example, Ethereum's white paper states that its contracts "should not be seen as something that should be 'fulfilled' or 'complied with'; rather, they are more like 'autonomous agents' that live inside of the Ethereum execution environment."[137] As this suggests, the language of "contracts" is a poor fit, because this sort of smart contract is not an exchange of promises or commitments. Creation of a smart contract—while setting certain events in motion—does not commit any party to do anything, or make any prospective promise.

Nevertheless, we believe that smart contracts are, at the conceptual level, still contracts.[138] Though they might not constitute promises per se, smart contracts are voluntary mechanisms that purport to alter the rights and duties of the parties. After all, not all traditional contracts are executory, either. A deal may still count as a contract even though it leaves nothing open to be done or performed. A conveyance, for example, is a contract that alters rights presently, and does not involve any further, open promises. Smart contracts similarly constitute present agreements without further promises to perform. The simple Bitcoin smart contract just imagined is more like a present but contingent conveyance than it is like an executory promise to pay.

Thus, the smart contract somewhat breaks down the traditional line between executory and executed contracts. Like the conveyance, there is no promise left to be performed. Unlike the conveyance, though, the smart contract does not transfer property at the time. It is neither executory, insofar as there is no action left to be performed, nor is it executed, insofar as the result is yet to be accomplished. This causes conceptual difficulty. Smart contracts are both committing to something in the future, but not exactly making a promise. As we discuss below,[139] this hybrid between ex ante commitment and ex post

---

137. *A Next-Generation Smart Contract and Decentralized Application Platform*, *supra* note 105; *see also Explainer: Smart Contracts*, *supra* note 14 ("[S]mart contracts are neither particularly smart nor are they, strictly speaking, contracts."); Leithaus, Comment to *Isn't Ethereum Just a DSL for the Blockchain?*, REDDIT.COM, https://www.reddit.com/r/ethereum/comments/31rnmh/isnt_ethereum_just_a_dsl_for_the_blockchain/ [https://perma.cc/44DG-ZV54] ("I now regret calling the objects in Ethereum 'contracts', [sic] as you're meant to think of them as arbitrary programs and not smart contracts specifically.").

138. For a more doctrinal analysis by an international law firm that reaches a similar conclusion, see NORTON ROSE FULBRIGHT LLP, *supra* note 12.

139. *See infra* Part II.B.3.

enforcement is novel.

In the end, though, this complication raises more questions about the conventional definitions of contracts than it does about whether smart contracts are contracts. There can be little doubt that smart contracts purport to alter the rights of the parties. The smart contract can explain, normatively as well as descriptively, why the Bitcoin belongs to one party and not the other. It constitutes an agreement between the parties, and not an idle one. That, we believe, is the essence of a contract. But it is an interesting conceptual observation—illuminated by the smart contract—that even yet-to-be-executed contracts need not create promissory obligations.

There is one final difficulty to overcome. Are smart contracts really agreements? After all, they are simply a chunk of code. Superficially, they may look nothing like a set of declarations in the form "Party X agrees to do such-and-such." In general, a legal contract requires mutual assent, a "meeting of the minds,"[140] meaning that both parties must have expressed assent to the contract.[141] That is, contracts require overt acts of assent.[142] Parties must engage in some expression that displays a shared understanding of the agreement, and a shared intent to bind themselves by its terms. Can smart contracts, simply a chunk of code in a blockchain, constitute such shared expression?

Nothing, so far as we can tell, prevents an expression of mutual assent from being formulated in code.[143] In general, mutual assent can take many forms, so long as it clearly implies agreement.[144] As Surden puts it, "[a]t a minimum, contract laws do not explicitly prohibit expressing contractual obligations in terms of data. More affirmatively, basic contracting principles actively accommodate data-oriented

---

140. *See, e.g.*, Krasley v. Superior Court, 161 Cal. Rptr. 629, 633 (Cal. Ct. App. 1980) ("The essence of a contract is the meeting of minds on the essential features of the agreement." (citations omitted)).

141. *See* 1 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 4.13 (Matthew Bender & Co. 2017) (1950) ("[A contract requires] mutual expressions of assent to the exchange. These expressions . . . are external symbols of the thoughts and intentions of one party, symbols that convey these thoughts and intentions to the mind of the other party.").

142. *See, e.g.*, Kitzke v. Turnidge, 307 P.2d 522, 527 (Or. 1957) ("The law of contracts is not concerned with the parties' undisclosed intents and ideas. It gives heed only to their communications and overt acts.").

143. We are assuming the parties have some understanding of what the code is intended to accomplish. As Scholz points out, they could essentially agree to agree, and let the algorithms do the rest. This may be the case with some computable contracts today, as in the case of high-frequency trading. *See* Scholz, *supra* note 33. However, this is not an inherent problem with smart contracts, whose key differentiation lies in complete enforcement.

144. *See* RESTATEMENT (SECOND) OF CONTRACTS § 4 & illus. 1 & 2 (AM. LAW INST. 1981).

representation."[145] In the present context, such data-oriented representations could easily include a blockchain. Where one party puts on the blockchain that assets of theirs will transfer to another party if some condition is satisfied, that seems to easily satisfy the requirement of an expression of assent.

This description in terms of a party putting the code on the blockchain does point to a wrinkle. Smart contracts, on Ethereum and presumably on other platforms, are by default unilateral, because only one party places them on the blockchain.[146] That is, the default involves one party specifying a transfer to another if certain conditions are met. Out of this default, one could approximate a bilateral or multilateral contract through the creation of two or more interrelated unilateral contracts.[147] But two unilateral contracts are not precisely the same as a bilateral contract.[148] Fashioning interdependent conditions in a way that would emulate a bilateral contract might be a challenge for smart contracts. But for the purposes of this Article, we will leave this issue aside and generally focus on unilateral contracts, because we think the same basic analysis would apply to bilateral contracts as they might be formulated as smart contracts.

To sum up, smart contracts are contracts. They are agreements to shift legal rights and responsibilities, no less than an agreement between two parties physically exchanging goods for payment over a counter. Their status as contracts might be obscured by the fact that the parties intend litigation to be impossible, may not make any promise, and may be expressed only in code. We suggest that these details do not alter the fact that smart contracts are, indeed, contracts in the important sense.

B. *What's New Here?*

Is a smart contract really any different than an ordinary one? The fact that smart contracts manifest agreements in machine-readable code is not novel, and neither is the possibility of automated performance based on rules-based judgments by computers. Both are

---

145. Surden, *supra* note 15, at 656.

146. *See* Raskin, *supra* note 23, at 314; Casey Kuhlman, Legal Approaches to Smart Contract Development (Apr. 9, 2014), https://www.youtube.com/watch?v=wnFqOfR5a7I#t=29m25s.

147. *Id.*

148. *See* Francesco Parisi, Barbara Luppi & Vincy Fon, *Optimal Remedies for Bilateral Contracts*, 40 J. LEGAL STUD. 245, 247 (2011) (illustrating from an economic perspective that, "contrary to intuition, the incentives faced in a bilateral contract are different from those that the parties would face if entering into two separate unilateral contracts").

features of data-oriented and computable contracts, which have been around for some time.[149] And just because smart contracts are being implemented today on the exotic technology of the blockchain does not mean they raise novel or interesting legal issues. As Judge Frank Easterbrook has argued, new technologies do not necessarily call for new legal doctrines, when fact patterns are fundamentally unchanged.[150]

We consider two perspectives suggesting that smart contracts are just technological manifestations of familiar contractual processes: escrow and self-help. One perspective focuses on the mechanism smart contracts use to ensure the execution of agreements, and the other perspective focuses on the way smart contracts employ technology to impose a remedy outside of the court system. Each perspective sheds light on the nature of smart contracts. However, neither perspective fully captures the way smart contracts operate. Smart contracts are distinct from preexisting forms because the digital code is not just a representation of the agreement; it is the agreement.

1. *Smart Contracts as Escrow*. One could view smart contracts as simple escrow arrangements with a digital veneer. In a typical escrow agreement, such as a house purchase, the buyer places funds in a special account. The escrow agent can only withdraw and disburse these funds to the seller after successful inspection and resolution of any other prepurchase issues. More generally, escrow suspends execution of a valid contract, and empowers a trusted third party to complete the process. Among other attributes, this approach overcomes the possibility of a prisoner's dilemma when the parties do not fully trust one another; otherwise, whichever one acted first would be vulnerable. The escrow arrangement substitutes mutual trust in the escrow agent for bilateral trust between the parties.

Smart contracts mimic the functionality of escrow. The smart contract code can place Bitcoins or other cryptocurrency tokens in a suspended state on the blockchain, where they cannot be spent until performance of the contract.[151] The execution step may be fully

---

149. *See supra* Part I.A.

150. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208. Judge Easterbrook was surely correct about this general point, but he may not have won the particular debate about the viability of cyberlaw. *See* Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, 69 FLA. L. REV. (forthcoming 2017).

151. *See* NARAYANAN ET AL., *supra* note 12, at 84–85 (explaining how Bitcoin scripts can

automated, or it may be implemented through multiple-signature verification, known as multisig.[152] In order for a multisig smart contract to execute, more than one party must provide its private encryption keys, indicating approval to execute the previously agreed-upon transaction.[153] If Abby wishes to purchase digital goods from Bob using a smart contract, the parties can use a multisig smart contract, for which the ultimate execution requires the digital signatures of two out of three parties, typically the buyer, the seller, and a trusted third party, such as an arbitrator. If the contract is satisfactory, the buyer and seller sign, executing the terms of the contract. If either party refuses, claiming breach, the arbitrator's signature decides the outcome.

Startups are already using the sophisticated capabilities of smart contracts to apply escrow in new ways. For example, CryptoCorp uses multisig for preclearance checks on Bitcoin transactions, similar to the way credit card companies decline transactions if the card has been subject to fraud or the payment exceeds preset limits.[154] BitHalo has implemented an escrow system for e-commerce transactions that avoids the participation of third parties entirely, by requiring collateral to be stored on the blockchain.[155]

The fact that smart contracts can implement escrow agreements does not make them identical to escrow. Conventional escrow depends upon a trusted firm or third party, because the parties themselves cannot serve as the escrow agents. A smart contract reliant on an arbitrator gives up the decentralized trust that the blockchain makes possible. Smart contracts performing only escrow-like functions are therefore more like standard data-oriented contracts. A true smart contract may employ the escrow-like mechanism of holding Bitcoins temporarily, but it does so through automated execution of scripts running on the network of computers maintaining the blockchain, without an escrow agent equivalent.

---

mimic escrow transactions); Cassano, *supra* note 93.

152.   *See* Ben Davenport, *What Is Multi-Sig, and What Can It Do?*, COIN CENTER (Jan. 1, 2015), https://coincenter.org/2015/01/multi-sig/ [https://perma.cc/W4VN-HTQT].

153.   *See* NARAYANAN ET AL., *supra* note 12, at 80.

154.   *See* John Villasenor, *Could "Multisig" Help Bring Consumer Protection to Bitcoin Transactions?*, FORBES (Mar. 28, 2014, 9:43 PM), http://www.forbes.com/sites/johnvillasenor/2014/03/28/could-multisig-help-bring-consumer-protection-to-bitcoin-transactions/ [https://perma.cc/QGG8-LAXB].

155.   *See* Diana Ngo, *BitHalo Releases Decentralized Escrow Client v2.1 to Rival PayPal, Western Union*, COINTELEGRAPH (Jan. 12, 2015), http://cointelegraph.com/news/113286/bithalo-releases-decentralized-escrow-client-v21-to-rival-paypal-western-union [https://perma.cc/JY2K-CVCB].

2. *Smart Contracts as Self-Help.* Researcher Max Raskin provides a different interpretation of smart contracts. He views them not as legal enforcement at all, but as a form of self-help.[156] To Raskin, "[a]utomated execution of a contract is a preemptive form of self-help because no recourse to a court is needed for the machine to execute the agreement."[157] He draws an analogy to starter interrupters, which are remote-controlled devices installed in cars to prevent them from operating.[158] A creditor can invoke the starter interrupter if the lessee of the car fails to pay. As Raskin notes, such devices are likely to be legal in most states, under the self-help repossession provisions for secured creditors at Section 9-609 of the UCC.[159] A smart contract could serve the same function, by refusing to authorize operation of the car unless the creditor receives payment.

Viewing smart contracts as self-help mechanisms accurately places the emphasis on the ex post enforcement function.[160] The blockchain can be used to record contractual provisions, execute contractual obligations, and perform intermediary functions like escrow, but so can garden-variety digital contracts. It is only when disputes arise, or when the remedies provided in the contract must be invoked, that smart contracts do something special. The algorithmic enforcement mechanisms, running automatically on the blockchain computing fabric, replace judicial enforcement.[161]

Self-help, traditionally, is a judicially supervised process.[162] Courts may restrain creditors from "disturbing the peace" to enforce their self-help rights, for example, or if a creditor's rights are inferior to other legal obligations, such as those of bankruptcy.[163] With a smart contract, there is no one to restrain, because the smart contract code is

---

156. *See* Raskin, *supra* note 23, at 306 ("Over the past few years, a group of innovators have begun designing computer technologies that bring self-help to the realm of contracts. They call these new contracts 'smart contracts.'").

157. *Id.* at 333.

158. *See id.* at 329–33.

159. *See id.* at 332.

160. *See* Zoë Sinel, *De-Ciphering Self-Help*, 67 U. TORONTO L.J. 31, 58–65 (2017) (explaining that self-help, properly understood, is responding to a committed wrong, and that ex ante measures are not properly considered self-help because they are not so responding).

161. *See supra* Part I.C.

162. *See* Sinel, *supra* note 160, at 66–67 ("[S]elf-help is a [limited] privilege . . . . Only the state's legal institutions (which include legally recognized agreements between two parties – that is, contracts) can effect [it] . . . . As such, self-help is not an alternative to the civil justice system but rather one small part of it.").

163. *See* Raskin, *supra* note 23, at 310.

immutable once embedded in the blockchain. A smart contract could even include terms that are illegal, unconscionable, or otherwise legally unenforceable.[164]

More deeply, the self-help model focuses on what smart contracts *do* to the exclusion of what they *say.* Functionally, the primary distinction between smart contracts and more limited data-oriented or computable contracts lies in enforcement. The smart contract, as we have explained, fully executes the agreement. It addresses the possibility of breach, not through the deterrent potential of judicial remedies, but by making breach practically impossible. The smart contract is not merely an accessory added to the end of the contractual process to mitigate the risk of breach.

Raskin's analogy between smart contracts and starter interrupters breaks down on closer examination. The starter interrupter is a mechanism introduced, after an agreement is reached, to enforce its terms; but, unlike smart contracts, this mechanism has nothing to do with the substance of the agreement. By contrast, a smart contract literally contains the terms of the agreement, transformed into machine-readable scripting code. The fact that the agreement is enforceable algorithmically, without the participation of legal institutions, is a commitment represented in the smart contract. Thus, the self-help model paints too limited a picture of smart contracts.

At the same time, the self-help model is too expansive. This analogy attributes functions to smart contracts that they do not actually perform; the smart contract itself does not perform the breach-limiting action, the blockchain and its computing nodes do. In the self-help model, by contrast, one party enforces the agreement consistent with, but *outside* the legal machinery of contract law. The smart contract is a component of a larger smart contract system, which ensures that, for example, the cryptocurrency tokens are transferred according to the contractual terms. Just as the state's ex post remediation role distinguishes a legal contract from an informal exchange of promises,[165]

---

164. Raskin's proposed solution to the possibility of illegal smart contracts is to suggest that some forms of smart contracts be prohibited through regulation. *See* Raskin, *supra* note 23, at 340. This begs practical questions about enforcement. Smart contract platforms on public blockchains, such as Ethereum and Bitcoin, are open-source software adopted voluntarily by networks of mining node operators. There is not a central smart contract administrator to regulate. And the fact that identity on the blockchain generally takes the form of digital signatures rather than real names means it may not be feasible even to identify the counterparty who created an undesirable smart contract.

165. *See infra* Part III.C.

the integration of specific contractual terms and a general enforcement infrastructure makes a smart contract smart. The distributed ledger software both instantiates the contractual terms and enforces the contractual obligations. These functions are distinguishable, but necessarily connected.

3. *Smart Contracts as Entire Agreements.* Both the escrow model and the self-help model explain smart contracts as technical mechanisms overlaid on the basic contractual process. Escrow does so to facilitate performance, while self-help provides a remedy for nonperformance. These tools may reduce transaction costs and thereby make contracting more efficient. They are not, however, strictly necessary to the outcome. Neither fully captures the essence of smart contracts, because both treat smart contracts as external enhancements to the contractual process. The distinctive aspect of smart contracts is not that they make enforcement easier, it is that they make enforcement unavoidable. In order to do so, they change the nature of the contract itself.

In Szabo's vending machine example, the physical security of the device is sufficient to make breach less attractive than compliance.[166] But alongside physical security, another element is at work in Szabo's example. The vending machine takes cash, which is a bearer instrument. Once the coins or bills are in belly of the machine, value has been transferred. No third parties need to be brought into the process to facilitate or secure the exchange. Szabo's example does not easily translate to other payment mechanisms, like checks or credit cards, which require a bank to validate the transaction. This step introduces transaction costs and delay, and it means the contracting process is no longer contained within the hardware and software of the vending machine. And, intermediary validation potentially changes the performance equation. The consumer can breach the agreement by instructing the bank to reverse the charge, even after receiving the product. At that point, the smart contract would no longer govern the relationship between the parties.

Cash works for a vending machine, but not for complex financial derivatives transactions, international supply chains, or major crowdfunding initiatives. Only a limited subset of transactions are sufficiently localized, low value, and low velocity for cash to be a viable

---

166.   *See supra* note 48 and accompanying text.

option.[167] For this reason, Bitcoin and other cryptocurrencies are very important for the growth of smart contracts. Bitcoin tokens are digital bearer instruments, functionally equivalent to cash, yet flexible and scalable in the manner of credit cards. A blockchain-based smart contract, like a cash transaction, therefore involves the complete exchange of value.

If I buy an e-book for my Kindle on Amazon.com, a complete transfer of value does not occur immediately. When I click the "buy" button, the company's computers transfer the e-book to my device, with associated digital rights to prevent additional copying, and they also process my credit card and debit my account. Yet, I am in a position to prevent a complete transfer of value, because I can still ask Amazon for a refund, or dispute the charge with the credit card company. This is possible because my contract with Amazon is executory—I have traded the e-book for the promise to pay my credit card issuer. Imagining the same exchange with a smart contract, by contrast, it is as though when I click the buy button, a drone picks up a stack of one-dollar bills from my house and flies them to Amazon. The contract fully executes with no human intervention. I can still dispute the transaction with Amazon, but now the contract is fully executed. Amazon has the cash; I am now asking them to return the money, rather than preventing them from receiving it.

Because the exchange of value is entirely contained in the smart contract environment, there is no need to look anywhere else. In other words, the contract *is* the scripting code that tells the network what to transfer and when. In the Amazon example, the site's computer system transfers the e-book and processes my credit card. Those machine instructions, however, are separate from my contract with Amazon, agreeing to exchange my payment information for a particular e-book.[168] If Amazon's programmers make an error and send me an entirely different e-book, there is no question that my contract with

---

167. Or, they are transactions the parties do not want traced because they are somehow illicit. Unsurprisingly, one of the major early uses of Bitcoin was for illegal transactions. *See* Joshuah Bearman, *The Rise and Fall of Silk Road: Part II*, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2 [http://perma.cc/4BCZ-LTBG] (recounting the story of a Bitcoin exchange commonly used for drug sales and other illegal activity); Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [http://perma.cc/6BKF-BKY7] (same).

168. There may be questions about what constitutes that contract. Perhaps it is a combination of what I saw on the shopping cart screen and Amazon's Terms of Service, or perhaps some judicial gap filling is required. Under no circumstances, however, is the contract exclusively the software code executed on Amazon's servers.

Amazon controls, rather than the software code the computer system uses to effectuate the contract.

For the smart contract, in contrast, everything beyond the code is just commentary. The code is a necessary part of the agreement itself, whereas Amazon's software code is just a tool to execute the human-made contract. For example, imagine that at the same time I place my order for the e-book on Amazon's website, I type up a written agreement for a different book and send it to an Amazon customer service agent, who countersigns it. In the event of a dispute, there would be an evidentiary question as to which version of the agreement controlled. In the smart contract context, such an inquiry would be meaningless. The smart contract has the entire life of the contract immutably embedded into its code, which leaves no room for a separate written agreement to specify the parties' intent. If a court concludes that some writing better reflects the parties' meeting of the minds, it would be powerless to invalidate the smart contract; it would have to find some way to reverse the transfer of value ex post.

The notion that smart contracts can supersede legal enforcement has been tested in the real world.[169] A group of developers associated with Ethereum created a distributed crowdfunding system in mid-2016 called "The DAO."[170] It was designed to implement the concept of DAO, in which corporate governance and operations are conducted automatically through smart contracts.[171] Users pledged Ether (the Ethereum cryptocurrency) in return for tokens that gave them authority to vote on projects to fund. Organizations seeking funding would sign up through another interface, and collect Ether if they received sufficient votes. Despite the novelty of the arrangement, Ethereum users pledged over $150 million in Ether in a matter of weeks after The DAO launched.[172]

Users signed up to participate in The DAO on a website that stated explicitly, in its terms of service, that the smart contract on the

---

169. We note that whether smart contracts can displace contractual enforcement is a different question than whether, as we consider in Part III, they can displace contract law.

170. Christoph Jentzsch, Decentralized Autonomous Organization to Automate Governance (unpublished manuscript), https://download.slock.it/public/DAO/WhitePaper.pdf [http:// perma. cc/SE35-Y8CC].

171. *See supra* note 125 and accompanying text.

172. Nathaniel Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalist*, N.Y. TIMES (May 21, 2016), http://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html?_r=0 [https://perma.cc/2GP2-H9N7].

Ethereum blockchain was the controlling legal authority.[173] Any human-readable documents or explanations, including those on the website, were "merely offered for educational purposes and do not supercede [sic] or modify the express terms of The DAO's code set forth on the blockchain."[174]

Within weeks of launch, something went wrong. A hacker took advantage of a bug in The DAO's code to siphon off over $60 million worth of Ether.[175] Although clearly an attempt at theft, the hack was executed through a series of smart contracts that were formally valid within the rules of The DAO. Even though the stolen funds were temporarily quarantined in an account, and not immediately disbursed, from the perspective of the smart contracting system, the transactions were perfectly legitimate. Even if a court ordered the funds returned, there was no one to carry out that order. Thus, there was no legal or technical way to recover them without undermining the entire system. Ultimately, the leaders of Ethereum project had to convince a majority of mining nodes to implement a "hard fork," which split the entire Ethereum blockchain into two incompatible paths.[176] Only through this dramatic step, which effectively killed off The DAO and undermined confidence in the Ethereum platform, could the stolen funds be returned.[177]

---

173. The DAO's original terms of service page, which was located at https://daohub.org/explainer.html, has been removed from the Web. For a contemporaneous quotation of the relevant language on the site, see Joel Ditz, *DAOs, Hacks and the Law*, MEDIUM (June 17, 2016), https://medium.com/@Swarm/daos-hacks-and-the-law-eb6a33808e3e [https://perma.cc/N9M5-F2GT].

174. *Id.*

175. Michael del Castillo, *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*, COINDESK (June 17, 2016, 2:00 PM), http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/ [https://perma.cc/3P4G-59MZ]; Nathaniel Popper, *A Hacking of More than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html?_r=2 [https://perma.cc/5NBQ-CFFN]. The varying valuations of the hack are due to the floating exchange rate between Ether and dollars.

176. Miners of one chain do not recognize the validity of blocks mined by the other clients, and vice versa, even though they may otherwise use exactly the same protocols. *See* Joseph Bonneau et al., *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies*, IEEE TECHNICAL COMMITTEE ON SECURITY & PRIVACY 104, 113 (May 18, 2015), http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf [https://perma.cc/SWM8-MQZC].

177. *See* Frances Coppola, *A Painful Lesson for the Ethereum Community*, FORBES (July 21, 2016, 1:54 PM), https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/#56d3a488bb24l [https://perma.cc/FRP2-7TDR]. The hard fork was considered a "nuclear option" because it was not just a reversal of transactions by the operator of The DAO; it broke the fundamental immutability of transactions on the Ethereum blockchain.

DUKE LAW JOURNAL   [Vol. 67:313

The DAO example shows the power of smart contracts, and also their limitations. Smart contracts seemed to be able to replace the legal system as an enforcement mechanism for The DAO users' contractual relationship with the crowdfunding system. However, doing so came at a significant cost. Because the only enforcement mechanism was the Ethereum network's computers executing the terms of The DAO software code, there was no way to distinguish between a legitimate string of transactions and one with malicious intent.

III. WHAT THEY TEACH US ABOUT CONTRACT LAW

As we have discussed, there are reasons to be skeptical about whether smart contracts can deliver all the hoped-for gains in efficiency and flexibility. But there is a much deeper, more theoretical reason to be skeptical of smart contracts. Even if the technology could deliver all that its proponents promise, it is not clear whether its implementation would be an improvement over courts or simply orthogonal. Put simply, the question is whether smart contracts could do what courts do, only better. We think not. Although we can see why some conclude otherwise, we think that contract litigation plays a role in our social system that smart contracts do not even purport to replicate.

Ostensibly, smart contracts remove the role of courts as enforcement agents. One might say that the contract enforces itself, or that the code itself enforces it. This means that parties no longer have the escape hatch of litigation. Once the smart contract is made, the machinery for its execution is unavoidably set in motion, ending the parties' opportunity to affect the transaction ex post.[178] This may be a bit of an overstatement. Parties can use multisig, for example, to

---

See Joon Ian Wong & Ian Kar, *Everything You Need to Know About the Ethereum "Hard Fork,"* QUARTZ (July 18, 2016), https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/ [https://perma.cc/B6DA-XC2L] ("If contracts held to be inviolable can effectively be overturned by a collective decision to run new software, what guarantee do financial institutions have that their transactions and funds are secure?"). A faction of the Ethereum community considered this such a breach of trust that it began mining the deprecated chain on which The DAO hack was not reversed, creating a duplicate token called Ethereum Classic. *See* David Z. Morris, *The Bizarre Fallout of Etherum's Epic Fail*, FORTUNE (Sept. 4, 2016), http://fortune.com/2016/09/04/ethereum-fall-out [https://perma.cc/ZK78-NCJX]. Broader questions about the legal or governance relationships among users, smart contract applications such as The DAO, and blockchain platforms such as Ethereum are beyond the scope of this Article. *See generally* Werbach, *supra* note 17 (discussing the governance implications of The DAO fiasco in connection with the trust architecture of the blockchain).

    178.   Note that this is consistent with the regular aim of business agreements to try to dictate remedies ex ante; for example, clauses pertaining to mandatory arbitration, choice of law/forum, disclaimer of incidental/consequential damages, among others.

maintain some control over the execution of the contract.[179] And in extreme cases such as The DAO hack, the entire blockchain could conceivably be forked if enough network nodes agreed.[180] Still, if smart contracts are to be a disruptive force in contracting, this potential turns on the ability to eliminate the possibility of breach and the resultant litigation to enforce.

Does this mean that smart contracts can replace courts in the adjudication of contract cases?[181] Courts, it might be argued, serve the function of enforcing contractual obligations. But, because courts serve this function in a costly and time-consuming way, technological advancement offers the possibility of making courts obsolete; surpassed by mechanisms that can enforce obligations, and serve the same function, with greater efficiency and customization.

Smart contracts thus offer a window into thinking about contract law at a theoretical level. Even if one were uninterested in the technology, smart contracts could illuminate foundational issues in the theory of contract. Their theoretical possibility, whether the technology can deliver or not, raises a pointed question about what function courts play when they adjudicate a contract case. Put another way, the basic question about whether smart contracts do what courts do, only better, introduces a reciprocal question about contract law more generally: Does contract law do what smart contracts aim to do? Taking smart contracts seriously is therefore a fruitful way to examine the function of courts and contract law.

In order to answer the question whether smart contracts can do what courts do, this Section describes three competing conceptions of what role courts play—or ought to play—in contract cases. Each view informs how its proponents think that smart contracts might interact with contract law. Ultimately, we argue that through the correct understanding of contract law, it is clear that smart contracts cannot supplant the role that courts play. Smart contracts are not, even conceptually, a replacement for judicial contract adjudication.

Our argument in this Section is bidirectional. Insofar as many readers may already intuitively grasp that smart contracts can, at best, avoid courts but cannot substitute for them, this Section provides the argument and reasoning to support that understanding.

---

179. NARAYANAN ET AL., *supra* note 12, at 62–63.

180. *See supra* note 175.

181. *See supra* notes 6–8 and accompanying text.

A. Contract Law as Enforcing Promises

According to one view, contract law provides legal enforcement for promises.[182] When a promisor makes a commitment to a promisee, this commitment, the promise, generates an obligation to do the thing promised.[183] Even without contract law, a moral obligation is created when one party makes a promise to another. While the exact source of this moral obligation is subject of philosophical dispute, there is little doubt that promises generate obligations.[184] Contract law, the argument goes, serves to strengthen and support these moral obligations by creating corresponding legal obligations. At its core, contract law binds promisors, not simply morally, but also legally.

The paradigmatic articulation of the view that contract law enforces promises is Charles Fried's 1981 book, *Contract as Promise*.[185] For Fried, the capacity to make promises is a form of freedom, allowing parties to bind themselves and thus shape their obligations.[186] By enforcing such voluntarily assumed obligations, the state supports the freedom of contracting parties.[187] The core idea is that contracts are binding, as the self-imposed obligations of contracting parties. Contracts, like promises, are the result of voluntary acts performed with the intent to place the actor under an obligation. The ability to bind oneself in this way—to assume an obligation voluntarily—is itself a form of freedom. But one need not share Fried's account of

---

182. *See generally* CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (1981) (grounding contract law in the morality of promises).

183. *See, e.g.*, *id.* at 8 ("By promising we transform a choice that was morally neutral into one that is morally compelled.").

184. Theoretical debate exits between convention-based views and reliance-based views. Conventionalist accounts understand promises as social conventions and understand their obligations as arising from the fact that failing to keep one's promise would do violence to a valuable social institution. *See, e.g.*, DAVID HUME, A TREATISE ON HUMAN NATURE 524–25 (L.A. Selby-Bigge ed., 1967). Fried's account of contract law appeals to such a convention-based account of promises. FRIED, *supra* note 182, at 11–17. Convention-based accounts face a problem explaining the sense that promissory obligations are owed directly to the promisee, which can be explained better by appealing to the interests of the promisee. *See* T.M. SCANLON, WHAT WE OWE TO EACH OTHER 295–327 (1998). For a picture of contract law built on such a reliance-based account of promissory obligation, see generally Joseph Raz, *Promises in Morality and Law*, 95 HARV. L. REV. 916 (1982) (reviewing P.S. ATIYAH, PROMISES, MORALS, AND LAW (1981)). For further discussion of this philosophical debate, see generally WILLIAM VITEK, PROMISING (1993) and Niko Kolodny & R.J. Wallace, *Promises and Practices Revisited*, 31 PHIL. & PUB. AFF. 119 (2003).

185. FRIED, *supra* note 182, at 17–21.

186. *Id.* at 8.

187. *Id.* at 21.

promissory obligations in order to think that contract law's purpose is to provide legal obligations that correspond to the moral obligations of promises.[188]

The essential idea is that promises are an important part of human life, and that contract law supports promising by offering legal recognition and enforcement. Contract law layers legal obligation on top of our moral obligations in order to bolster them. By making it the case that a party must, legally, do what it has promised, we affirm that people ought to do what they promise, and we thereby affirm the institution of promising. The point of contract law, then, is to help ensure that people are truly bound by their promissory commitments.

From this perspective, contract law might appear incrementally more successful the more it affirms that promisors must do as they have promised. In this light, elements of contract law that diverge from ensuring that parties keep their promises may seem troubling.[189] Particularly, it may appear problematic that contract law generally imposes only expectation damages, rather than specific performance.[190] Specific performance more closely matches our moral obligation to do the thing promised.[191] Insofar as the point of contract law is to strengthen and affirm our moral obligations, and insofar as our moral obligations are to do as we have promised, then contract law should aim to align morality and legal obligation.

If one holds this conception of contract law's function, then smart contracts may seem like an appealing alternative to court-based contract law. Courts exert legal force upon us to do as we have promised, thus strengthening our voluntarily assumed commitments. But legal force is a relatively clumsy mechanism. If we want people to

---

188. *See generally, e.g.*, T.M. Scanlon, *Promises and Contracts*, *in* THE THEORY OF CONTRACT LAW 86 (Peter Benson ed., 2001) (defending a view of contract law based on the importance of providing assurance to another that promising allows); Daniel Markovits, *Contract and Collaboration*, 113 YALE L.J. 1417 (2004) (defending a view of contract law based on the community created between promisor and promisee).

189. *See, e.g.*, Seana Valentine Shiffrin, *The Divergence of Contract and Promise*, 120 HARV. L. REV. 708, 749 (2007) (noting the aim of "advanc[ing] an accommodationist approach that renders the norms of interpersonal morality relevant to the shape of law" and "deploy[ing] this approach to sound some alarms about the divergence of promise and contract, particularly with respect to contract's remedial doctrines").

190. *Id.* at 724 ("The law . . . fails to use its distinctive powers and modes of expression to mark the judgment that breach is impermissible as opposed to merely subject to a price.").

191. *Id.* at 722 ("Contract law would run parallel to morality if contract law rendered the same assessments of permissibility and impermissibility as the moral perspective, except that it would replace moral permissibility with legal permissibility and it would use its distinctive tools and techniques to express those judgments.").

do as they have promised, then a mechanism that automatically and completely ensures performance may look like a triumph, at least to the extent that it does not come at the expense of other freedoms.[192]

Smart contracts, according to this line of thought, are like specific performance on steroids and without the state's coercive machinery. Smart contracts make it the case that promisors will do precisely what they promise, radically strengthening promises. If this is the point of judicial contract enforcement, then it looks like smart contracts offer a superior technology, and smart contracts would leave judicial enforcement essentially obsolete.

Of course, there is room for concern within this picture of contract law as enforcing promises. First, one might suggest that smart contracts, by making performance inevitable, are no longer promises at all.[193] If so, smart contracts would not reinforce the practice of promising. Whereas contract law supports promising by giving promisors legal reasons to perform, smart contracts do away with the need for reasons altogether, and fail to support the moral agency involved in promising. Pragmatically, it may not be obvious why we should value promising, apart from the reliable commitments that promising enables.[194] But, assuming we should value promising for other reasons, then smart contracts highlight the fact that contract law

---

192. One reason to disfavor specific performance, even while recognizing that it would be preferable in terms of accurately corresponding with the underlying moral commitment, is that the coercion involved with implementing such a remedy would be too burdensome. This reason is often noted particularly with regard to personal service contracts. *See, e.g.*, 12 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 65.25 (Matthew Bender & Co. 2017) (1950) ("A second reason [against specific performance] is that we have a strong prejudice against any kind of involuntary personal servitude. We insist upon liberty even at the expense of broken promises."). It is sometimes even suggested that specific performance might violate the constitutional prohibition on slavery, though the merits of this constitutional claim is questionable. *See* Nathan B. Oman, *Specific Performance and the Thirteenth Amendment*, 93 MINN. L. REV. 2020, 2025 (2009).

193. One must be cautious not to overstate the point though. Smart contracts do require a voluntary act by the contracting agent at the outset.

194. In any event, a significant further argument would be needed here. It's not transparent that a hypothetical world in which making a promise produced an unfailing compulsion to do the thing promised would be a morally impoverished world. If smart contracts make our world more like this, then they would not bolster agents' choices to keep their promises. But it's not clear why we should care about *that*.

One obvious rationale for creating reasons, as opposed to action directly, would be to respect the freedom or agency of others. I can give you reasons to raise your right hand, but I ought not simply thrust your hand upwards. But this rationale does not apply in as straightforward a way when it is one's own action, as contracting involves. If what I aim to do is to get myself to act, what I may seek is motivation rather than merely reasons.

is about creating or supporting reasons to fulfill our moral obligations, and not only about creating reliable consequences.

Second, one might think that contract law is not only about supporting promises, but about the community or state being the entity lending support. On this view, it is essential that contract law strengthens promising through a political medium. In a contract case, we collectively express our affirmation of an obligation and lend our resources to enforcing that obligation.[195] Smart contracts, by contrast, would strengthen promissory obligations without this state involvement. Of course, to their proponents, this is a key feature of smart contracts.[196] But, to others, this might be a bug. Even though smart contracts would strengthen promises, it would be problematic that this strength fails to come from the political community. Smart contracts would thus raise worries similar to those expressed toward private arbitration or penalty clauses.[197] That is, one might worry that something is lost simply by transferring the power away from the political community.

Leaving aside worries like these, the general point is that if the function of contract law is to strengthen moral obligations to keep promises by adding legal coercion, then smart contracts seem well suited to supplant this function. In short, if contract law is about making people keep their promises, then smart contracts look like they can do that job even better than courts.

---

195. *See, e.g.*, Seana Valentine Shiffrin, *Paternalism, Unconscionability Doctrine, and Accommodation*, 29 PHIL. & PUB. AFF. 205, 221 (2000) ("[T]he institution of contract is an institution in which the community assists people who make agreements by providing a measure of security in those agreements.").

196. *See* Popper, *supra* note 49.

197. *See, e.g.*, Owen M. Fiss, *Against Settlement*, 93 YALE L.J. 1073, 1075 (1984) ("I do not believe that settlement as a generic practice is preferable to judgment or should be institutionalized on a wholesale and indiscriminate basis. It should be treated instead as a highly problematic technique for streamlining dockets."); Seana Valentine Shiffrin, *Remedial Clauses: The Overprivatization of Private Law*, 67 HASTINGS L.J. 407, 411 (2016) (noting that remedial clauses are objectionable since they "displace the public's role in determining the content of an important area of law and objectionably displace the judiciary's role in providing fair and impartial judgments about the public significance of legal wrongs"). There is a significant difference for smart contracts, however. Arbitration and penalty clauses ultimately depend on judicial sanction, so that state power is ultimately at issue. Smart contracts, in contrast, do not implicate state authority in this way. So, whereas arbitration and penalty clauses necessarily implicate state power and thus arguably make the political community complicit in their results, it is harder to make such a case about smart contracts.

B. *Contract Law as Voluntary Liability*

A second view of contract law conceives it as a method to create legal liability voluntarily, in a way that is not necessarily connected to morality or promising. According to this view, contractual obligations need not correspond to moral obligations.[198] Instead, contractual obligations can be fashioned where it is in the interest of parties to create them. By creating legal liability, parties can create a distinctive obligation that can serve any number of purposes, from enhancing agency[199] to facilitating efficient transactions.[200]

There are three key elements in this second view. First, contracts—as opposed to promises—involve parties agreeing to legal liability if they fail to perform. The crucial element of contract law is that certain agreements are legally binding; that is, they are subject to agreed-upon legal sanctions for breach. But whether and how any agreement is legally binding is ultimately up to the parties.[201] Rather than understanding legal liability as parasitic on existing moral obligations, this view sees legal liability as the elective creation of the parties involved.

Second, the legal obligations of contract reflect parties opting into liability. Insofar as parties opt into a system of legal penalties, the legal obligations describe those actions to which a legal sanction will attach.[202] Thus, by making it the case that a party will face a sanction

---

198. *See* Jody S. Kraus, *The Correspondence of Contract and Promise*, 109 COLUM. L. REV. 1603, 1617 (2009). As Professor Kraus explains:

> When a correspondence account insists on enforcing a promise made by a promisor who intended it not to be legally binding, it paradoxically purports to justify a legal obligation on the ground that it enforces a moral responsibility derived entirely from the individual's free will, even though legally enforcing that obligation violates the will of the very same individual whose autonomy the moral obligation is supposed to vindicate.

Id.; *see also* Michael G. Pratt, *Contract: Not Promise*, 35 FLA. ST. U. L. REV. 801, 809–10 (2008) ("The objection to the claim that contracts are promises, which I have been pressing, exploits the fact that at least some contractual undertakings generate nothing like the moral obligation to perform that attaches to the making of a binding promise.").

199. *See, e.g.*, Robin Kar, *Contract as Empowerment*, 83 U. CHI. L. REV. 759, 761 (2016) ("[C]ontract law aims to empower people to use promises as tools to influence one another's actions and thereby to meet a broad range of human needs and interests.").

200. *See, e.g.*, Charles J. Goetz & Robert E. Scott, *Enforcing Promises: An Examination of the Basis of Contract*, 89 YALE L.J. 1261, 1266 (1980) (arguing that allowing people to bind themselves legally improves utility by shaping and encouraging promise-making activity).

201. *See, e.g.*, Randy Barnett, *A Consent Theory of Contract*, 86 COLUM. L. REV. 269, 319 (1986) (offering a theory of contract in which "[c]ontractual enforcement . . . will usually reflect the will of the parties").

202. On this view, it would be incoherent to imagine parties agreeing to create a legal

for failing to perform, that party thereby generates its own obligation to perform.

Third, because contracting is about parties choosing to attach legal consequences to future actions, questions of contract law should address how to determine what the parties intended, or would have chosen, ex ante.[203] The basic question is what the parties would want, perhaps subject to certain additional nuances.[204] A range of contract doctrines can then be explained as default rules, presumed to be what most parties would want unless they explicitly indicate otherwise.[205] Contract law, then, is fundamentally about enabling transactional activity, by creating a system in which one can voluntarily bind oneself through opting into flexible and predictable consequences for breach.

If this is what contract law does, then smart contracting again looks like it could supplant it. According to this second view, the fundamental purpose of contract law is allowing people to create reliable consequences, enabling them to shape their behavior. The essential feature of contracts is the communication of information about what will happen in the future.[206] Efficient or agency-enhancing transactions can only take place if such communication is intelligible and trusted.

Smart contracts offer the possibility of highly reliable

---

obligation to φ and yet attaching no ex post legal consequences to a failure to φ. The legal obligation necessarily and completely reflects that fact that some consequence attaches. This does not mean that obligation and the consequences are one and the same. Any given obligation might have a range of legal consequences.

203. *Cf.* Goetz & Scott, *supra* note 200, at 1264 ("It is important to emphasize that the proper focus here is on prospective effects, that future promising is the behavior to be influenced by the rules summarized above.").

204. *Cf.* Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 91 (1989) ("We suggest that efficient defaults would take a variety of forms that at times would diverge from the 'what the parties would have contracted for' principle.").

205. *See, e.g.*, Kraus, *supra* note 198, at 1648 (noting that "majoritarian default rules respect personal sovereignty—by maximizing the likely convergence between individuals' promissory obligation and their subjective intent—and by increasing the benefits and reducing the costs of exercising the positive individual liberty to undertake self-imposed moral obligations"); *cf.* Charles J. Goetz & Robert E. Scott, *The Limits of Expanded Choice: An Analysis of the Interactions Between Express and Implied Contract Terms*, 73 CALIF. L. REV. 261, 263 (1985) ("Our framework departs from the conventional view that state-supplied contract clauses are means merely of reducing negotiating and other resource costs; it focuses instead on the value of implied terms as widely useful, predefined signals that reduce the incidence of certain identifiable types of formulation errors.").

206. *See* Goetz & Scott, *supra* note 200, at 1267 ("[T]he promisor informs the promisee about the proposed future receipt of a benefit. The promise itself is merely the production of a piece of information about the future.").

communication about future outcomes. This is true in two ways. First, because the agreed-upon result occurs automatically, uncertainty about performance, and about judicial recognition, disappears. A promisee no longer needs to wonder whether the promise will be kept, or whether a court will recognize the breach. Second, because the code is itself the contract, provisions are laid out in precise, operational terms by definition, to a heightened degree as compared to traditional contract language.

In a well-functioning smart contract, the contract necessarily answers interpretive questions in determinative ways. In short, if contract law exists to facilitate reliance through the ability to opt into predictable future consequences, then smart contracts seem to serve this function even more seamlessly. If contract law is a commitment mechanism, then smart contracts seem to be a superior commitment mechanism.

Again there is room for concern. Specifically, one might worry that the ex ante information costs to determine all contingencies could make smart contracting overly costly. While this is undoubtedly a significant concern, it is ultimately a practical rather than theoretical objection. If smart contracts came with an array of well-understood default rules,[207] that could mitigate the ex ante information costs. To the extent that they persist, it would be a contingent matter to decide in what situations the information costs outweigh the gains in certainty. Smart contracts would, at least some of the time, be a better technology than ex post contract litigation. And this reflects the fact that, on this view, smart contracts and contract law serve the same underlying function.

C. *Contract Law as Ex Post Adjudication*

We believe that smart contracts are not, even theoretically, a substitute for contract law. Consequently, we believe that the above views about contract law's function, which appear to suggest that smart contracts could replace contract law, are unsatisfactory. These two arguments are mutually reinforcing: one can see the incommensurability of smart contracts and contract litigation by attending to the true function of contract law; and one can see the inadequacy of the above views about contract law by attending to the way in which smart contracts cannot serve the same function as

---

207. Presumably part of any smart contracting platform—and much of what competing platforms might compete over—would be supposedly majoritarian and efficient default rules.

contract law.

Both views of contract law described thus far assume an ex ante perspective that focuses on how contract law shapes our deliberations and motivations. That is, for both views, contract law is about giving us reasons to act. On the first view, contract law shapes our deliberation by supplementing our moral obligations with corresponding legal obligations. As such, contract law gives us an additional legal consideration in favor of keeping our promises. On the second view, contract law allows us to generate obligations that will shape our deliberations going forward, by electing to impose liability for some actions. As such, contract law creates motivations to comply, which need not correspond with our moral reasons, through the imposition of potential legal liability.

If one holds the second, motivation-creating view of contract law, then it is natural to see smart contracts as supplanting contract law. After all, why create motives for action when one can ensure the action itself?[208] If contract law is about facilitating our actions going forward, then the smart contract seems like an appealing innovation.

But that is not what contract law is about. Contract law does not exist to alter our reasons going forward—though it surely does that. Rather, it exists to adjudicate the justice of a situation ex post.[209] It is backward looking. Its basic function is to decide whether one party has wronged another party by failing to perform a promised action. That is, contract law is a fundamentally remedial institution, not aimed at creating new reasons to perform, but aimed at resolving disputes, taking those reasons as already given. One can see this backward-looking, remedial character in the way that contract law waits for breach, waits for an aggrieved party to bring forward a complaint, and even then rarely orders conduct.[210] We suggest that contract law is not about creating forward-looking reasons, because other mechanisms might serve that purpose equally or better.

---

208. The same thing might be said about creating reasons for action, *see* Shiffrin*, supra* note 189, at 749, but there are significantly more questions here. It may be that there is a value to an institution that creates reasons—causes a certain kind of normative engagement—apart from its ability to create motivation. We leave that possibility very open. But, if so, then this again highlights the inability of smart contracts to supplant contract law.

209. *Cf.* RESTATEMENT (SECOND) OF CONTRACTS ch. 16, intro. note (AM. LAW INST. 1981) ("The traditional goal of the law of contract remedies has not been compulsion of the promisor to perform his promise but compensation of the promisee for the loss resulting from [the] breach.").

210. *See generally* Cornell, *supra* note 19 (arguing that rather than enforcing promises and their obligations, contract law enforces complaints against promissory wrongs).

A simple example can illustrate the differences between the three views. Suppose Abby promises Bob that she will pay him back the money that he is considering lending to her. By promising, Abby creates a moral obligation. She now has a special sort of reason to pay the money back. These points about obligation and reasons are true independent of the law. What might contract law add? On one view, it might add an additional obligation—a legal obligation—that corresponds with the moral obligation. So, Abby's moral reasons to pay the money back would now be bolstered by parallel legal reasons or legal motivations. On another view, contract law might add an option for an additional liability. By promising, Abby has subjected herself to moral responsibility, and in doing so, she has created reasons to perform by opening herself up to moral sanctions. In addition, contract law allows her, if she would like, to subject herself to even more accountability—legal accountability. Thus, she could create more, or different, motivations to perform by opening herself up to a new set of sanctions. The difference between these two views is that on the first, but not the second, the legal obligations correspond with the moral obligations. But, according to both answers, contract law adds additional obligations and thus additional motivation to pay Bob back.

But an altogether different answer about what contract law adds is the view that contract law creates a forum to determine what happens if Abby does not perform.[211] On this view, contract law does not change anything about Abby's obligations. Those were complete the moment that she promised—she has reason to pay the money back because she promised to pay the money back.[212] Contract law did not make it that case that Abby *had to* do anything; Abby herself made it the case that she *had to* do something. Contract law adds something ex post to deal with failure. It is not about ensuring that she performs, but about responding if she does not. Contract law enables an avenue for Bob to

---

211. This idea appears to be an element of recent civil recourse theory. *See generally* Nathan B. Oman, *Consent to Retaliation: A Civil Recourse Theory of Contractual Liability*, 96 IOWA L. REV. 529 (2011) (noting that contract law helps facilitate social welfare by holding individuals accountable without the need for recourse to private violence); Benjamin C. Zipursky, *Civil Recourse, Not Corrective Justice*, 91 GEO. L.J. 695 (2003) (arguing that contract law is a form of corrective justice designed to make aggrieved parties whole). One need not accept all aspects of current civil recourse theory to maintain that contract law is not fundamentally about the creation of reasons ex ante.

212. Of course, this reason may have certain special characteristics—in particular, it may be content-independent and it may be exclusionary. *See* JOSEPH RAZ, MORALITY OF FREEDOM 35 (1986) ("A reason is content-independent if there is no direct connection between the reason and the action for which it is a reason.").

complain if Abby does not fulfill her obligations.

One might think that this avenue for complaint feeds back into the reasons that Abby has to perform. And, in a way, that is true. Abby does get a reason to perform from contract law—specifically, she will be liable to a complaint from Bob if she does not. But that is an indirect, independently empty reason, because it is a new reflection of the reason that she already had. It would be almost absurdly circuitous to think that contract law's primary function was about shaping reasons in such a redundant way. It is much more straightforward to see contract law as fundamentally about adjudicating the wrongs of broken agreements, and the function of creating reason or motivation as incidental.

When one views contract law in this way, then it is apparent that smart contracting does not even purport to do what contract law does. The two have fundamentally different objectives. Smart contracting functions to ensure action. Contract law functions to recognize and remedy grievances. Smart contracts could not—even in theory— replace contract law. At best, smart contracts might reduce the need for contract litigation. But that would not mean that smart contracts serve the same function in a superior fashion.[213] Rather, shifting to smart contracts would mean a shift to an altogether different mode of interaction, and one not clearly superior.

IV. SMART CONTRACTS IN PRACTICE

If smart contracts do something fundamentally different than contract law, does that mean legal scholars can safely ignore them? Perhaps it was all just a misunderstanding, borne out of Szabo's unfortunate choice of terminology two decades ago. If he had called his idea "intelligent agents" or "virtual vending machines," perhaps there would be no reason to examine the legal implications further, but we believe there are still reasons. Our conclusion, that smart contracts are orthogonal to contract law, does not end the inquiry. Smart contracts will be used in situations otherwise subject to contract, and will still be nominally subject to contract law. Problems are likely to

---

213. To think otherwise would be like thinking that text messaging supplants the function of reading facial expressions insofar as the complete adoption of the former might make the latter unnecessary. *Cf.* Jeffrey Kluger, *We Never Talk Anymore: The Problem with Text Messaging*, TIME (Aug. 16, 2012), http://techland.time.com/2012/08/16/we-never-talk-anymore-the-problem-with-text-messaging/ [https://perma.cc/AGN6-AVAG] ("Habitual texters . . . don't get to practice the art of interpreting nonverbal visual cues.").

arise. These in turn will produce responses with real consequences, both for the parties involved, and for the development of contract law.

Proponents of smart contracts argue they will eliminate the friction of legal disputes.[214] This view is overly optimistic.[215] While the potential benefits of smart contracts are substantial, the potential problems are significant as well. There is a Frankenstein dimension to a smart contract: an instrument that fuses something innately human, entering into and enforcing agreements, with something mechanical, derived from scientific experiments. Science fiction authors since Mary Shelley have warned of the consequences of such cyborgs.[216] Perhaps the benefits of smart contracts will exceed the costs. Perhaps the benefits can be magnified, or the costs minimized. We should, nonetheless, carefully assess both sides of the ledger.

Contract law is, of course, far from perfect. Yet by switching from the ex post adjudication of contract to the ex ante reduction of agreements to software code, smart contracts will in some cases merely shift problems rather than eliminate them. Smart contracts are likely to face two kinds of problems, practical and doctrinal. These difficulties will create pressure for responses. Some traditional solutions can be grafted onto the technical apparatus with limited disruption. Others, however, will involve reintroduction of law. They may even lead to greater regulatory involvement in contract.

---

214. *See, e.g.*, TAPSCOTT & TAPSCOTT, *supra* note 8, at 109 ("[T]hrough smart contracts . . . [c]ompanies can program relationships with radical transparency . . . . And overall, like it or not, they must conduct business in a way that is considerate of the interests of other parties. The platform demands it."); Cassano, *supra* note 93 ("Someday, these programs may replace lawyers . . . ."); Andrew Keys, *Memo from Davos: We Have a Trust Problem. Personal Responsibility and Ethereum Are the Solutions*, CONSENSYS BLOG (Jan. 19, 2017), https://media.consensys.net/memo-from-davos-we-have-a-trust-problem-personal-responsibility-and-ethereum-are-the-solutions-19d1104946d8#.c46zvkcks [https://perma.cc/4AQC-T4SW] ("It is early days, and there will surely be the need of attorneys, auditors, and regulators to learn, educate and facilitate smart contracts, but the process will become much more automated, intermediaries will be removed and the cost of trust will plummet.").

215. How widespread litigation will be is an open question. There is also the question of whether aggrieved parties in smart contract arrangements can effectively litigate. As with any transactions on a blockchain, smart contracts designate parties based on cryptographic signatures. The counterparty may be anonymous, or in a different jurisdiction.

216. *See generally* MARY WOLLSTONECRAFT SHELLEY, FRANKENSTEIN, OR, THE MODERN PROMETHEUS (1818) (highlighting the dangers that result from creating a new being). *Cf.* Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks,* 11 MINN. J. L. SCI. & TECH. 573 *passim* (2010) (describing firms in the securities industry increasingly dependent on information technology as "corporate cyborgs").

A. *Imperfections of Algorithmic Enforcement*

There are significant practical limitations in replacing human enforcement of agreements with software running on the blockchain. Things simply do not always go according to plan.[217] Anyone who has seen an error code on their computer knows that sophisticated software-based systems are imperfect. Even if the underlying blockchain consensus mechanisms are reliable, the smart contract applications running on top of them may not be.[218] The failure of The DAO should be a cautionary note for smart contract developers.[219]

Even without bugs, there are reasons to doubt smart contracts will always operate as desired. First, they require reduction of human-readable language to machine-readable code. This limits their scope to those subjects and activities that can readily be specified.[220] For example, a contract to unlock my connected car upon presentation of a certain cryptographic key can easily be encoded through a programming language such as Ethereum's Solidity. The network address for the car lock, the desired key, and the action to be taken, are all subject to precise definition. At the other extreme, some contractual terms simply cannot be expressed through formal logic, because they imply human judgment. A machine has no precise way to assess whether a party used "best efforts," for example.[221]

---

217. *See* Scholz, *supra* note 33 ("First, the use of algorithms to determine terms in a contract creates the possibility for emergence, that is, results that are not and indeed could not be foreseen by the algorithm's creator. This creates situations where the entity responsible for the algorithm does not know how it works and cannot predict its behavior.").

218. Peter Vessenes, cofounder of the Bitcoin Foundation, reviewed publically available Ethereum smart contracts and estimated there were 100 errors per 1000 lines of software code. *See* Peter Vessenes, *Ethereum Contracts Are Going To Be Candy for Hackers*, VESSENES (May 18, 2016), http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/ [https://perma.cc/6ARK-9NGV]. Even for commercial software, the industry average is as high as 25 errors per 1000 lines of code. *See* STEVE MCCONNELL, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION 521 (2d ed. 2004).

219. *See supra* notes 173–77 and accompanying text.

220. *See* Surden, *supra* note 15, at 682–83.

221. A computable or smart contract could be encoded with an algorithm to evaluate such imprecise terms. Human courts and juries often use proxies, formulas, or framing mechanisms to evaluate concepts such as reasonableness or best efforts. At best, however, this reduces but does not eliminate the grey areas around imprecise terms. And even when it offers a precise answer, something is lost in the process in the conversion from analog to digital.

The other way smart contracts can address non-machine-encodable terms is to reintroduce humans. The oracles that the smart contract code references to assess performance may be powered by people rather than just reporting facts in the world. Or the smart contract may incorporate an arbitrator who can resolve uncertain cases in favor of one party or the other through the multisig mechanism. *See supra* note 152 and accompanying text. At some point,

Building a computerized system able to interpret smart contracts like humans can is effectively a challenge for artificial intelligence.[222] And that challenge is unlikely to be solved any time soon.[223] Despite great advances in machine learning, computers do not have the degree of contextual, domain-specific, subtle understanding required to resolve contractual ambiguity. In this regard, smart contract platforms like Ethereum are also vastly less sophisticated than state-of-the-art artificial intelligence systems like IBM's Watson.

Even if the smart contract operates exactly as designed, it may produce suboptimal results, either in the minds of one or both parties, or as a matter of economic efficiency, because it is fixed. Sometimes, for example, nonperformance is the desirable outcome. Much has been made of the idea of efficient breach.[224] If a builder contracts with a carpenter to make custom woodwork for a new home, but notifies the carpenter that the home will not be built before initiation of that work, nonperformance and compensation to the carpenter may be the best result. One interpretation is that contract law is designed to facilitate such nonperformance, assuming the legal default rules for contractual remedies stood behind the parties' negotiation.[225] But, one need not accept the theory that the law sanctions efficient breach to appreciate that the law does not lock parties into performance.[226]

---

however, doing so transforms the smart contract into a conventional contract with an arbitration clause, eliminating the alleged benefits of the approach.

222. Steve Omohundro, *Cryptocurrencies, Smart Contracts, and Artificial Intelligence*, 1 AI MATTERS 19, 20 (2014), http://delivery.acm.org/10.1145/2690000/2685334/p19-omohundro.pdf ?ip=152.3.34.48&id=2685334&acc=ACTIVE%20SERVICE&key=7777116298C9657D%2E18C 4EEC63BFE39A6%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&CFID=814801535&CF TOKEN=37250381&__acm__=1506721336_f72d6efe11d8ca2344c4f38501c0dee5 [https://perma.cc/T46Y-QCKH].

223. "The conventional view has been that the automation of contract monitoring or compliance is beyond the capability of contemporary technology." Surden, *supra* note 15, at 632 (citing ENRICO FRANCESCONI, SIMONETTA MONTEMAGNI & WIM PETERS, SEMANTIC PROCESSING OF LEGAL TEXTS: WHERE THE LANGUAGE OF LAW MEETS THE LAW OF LANGUAGE 60–62 (2010)); Symposium, *Legal Reasoning and Artificial Intelligence: How Computers Think Like Lawyers*, 8 U. CHI. L. SCH. ROUNDTABLE 1, 19 (2001).

224. *See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 13–14 (1998); Robert L. Birmingham, *Breach of Contract, Damage Measures, and Economic Efficiency*, 24 RUTGERS L. REV. 273, 284 (1970) ("Repudiation of obligations should be encouraged where the promisor is able to profit from his default after placing his promisee in as good a position as he would have occupied had performance been rendered.").

225. *See* Steven Shavell, *Is Breach of Contract Immoral?*, 56 EMORY L.J. 439, 452 (2006) ("[B]reach could be immoral or moral. To know which is the case, we have to inspect the reasons for breach and the knowledge of the party committing breach.").

226. *See* Cornell, *supra* note 19, at 1175 ("Contract law does not offer a norm against breach of contract. This is not—as the theory of efficient breach would suggest—because contract law

The general lesson is that facts may change between the ex ante specification of contract rights and the ex post adjudication of legal effects. Parties to smart contracts can try to hedge against such changes by incorporating qualifying language or *force majeur* clauses, but those kinds of imprecise terms are difficult to specify in computer code. In other cases, parties may wish to advantageously alter a contract prior to performance. Under standard contract law, such modifications are unproblematic.[227] For smart contracts, such modifications pose a difficulty. Upon agreement, a smart contract is locked in place and secured by pledged cryptocurrency. To enable an intermediate step before execution, the smart contract code would need to incorporate the possibility of modification explicitly. As a technical matter, this would increase the complexity of the process. It would also introduce the kinds of difficulties already described about how to express complex ideas in code, like when and how parties can modify the set terms of a smart contract.

As the literature on relational contracts recognizes, contracts are often more than a one-time interaction between parties, followed by performance or judicial resolution of a dispute.[228] Instead, contracts are elements of ongoing relationships.[229] Both the parties and the courts view the contract in light of social and relational norms. Ex ante, parties to a relational contract must anticipate later renegotiation, and ex post, courts must determine how to fill gaps in the agreed-upon contract.[230] Smart contracts attempt to atomize the contractual process. They formally strip away the time dimension of interactions between the parties, and the uncertainties of future judicial resolution. Yet, smart contracts bind real people, who have real relationships, and their performance unfolds over time. This makes it impossible to avoid some of the messiness that attends traditional contracts.

B. *Doctrinal Concerns*

Contract law developed over centuries to account for situations that arise in the execution of agreements. Through the inductive

---

judges breach of contract permissible when the costs are high enough. Contract law simply does not determine permissibility.").

227.   *See* RESTATEMENT (SECOND) OF CONTRACTS § 89 (AM. LAW INST. 1981).

228.   *See* Ian R. Macneil, *Contracts: Adjustment of Long-Term Economic Relations Under Classical, Neoclassical, and Relational Contract Law,* 72 NW. U. L. REV. 854, 900–01 (1978).

229.   *See, e.g.,* Macauley, *supra* note 91.

230.   *See* Eric A. Posner, *A Theory of Contract Law Under Conditions of Radical Judicial Error*, 94 NW. U. L. REV. 749, 751 (2000).

process of the common law, courts evolved solutions to novel problems. Upon closer examination, many of these rules are in tension with smart contracts' mechanism of automatic, irrevocable enforcement.

At a basic level, a smart contract can meet the legal requirements for a valid and enforceable common law contract: offer, acceptance, consideration, capacity, and legality.[231] But a host of potential problems lurk beneath the surface. At virtually every turn, smart contracts might operate in ways contrary to legal contracts. That is, although smart contracts may be legal contracts, they may also fall victim to almost every legal deficiency. Nothing in a smart contract ensures a true meeting of the minds; nothing ensures consideration; and so on. Below, we describe a number of ways that smart contracts might operate problematically, and contrary to the law of contracts.[232]

1. *Problems with Meeting of the Minds.* A smart contract is computer code representing an agreement between two or more parties, so one question might be whether it truly represents a meeting of the minds. Computers, after all, do not have minds, at least not outside the realm of science fiction. But this objection is quickly overcome. In modern contract law, offer and acceptance are evaluated objectively;[233] that is, we allow evidence that both parties intend to be bound, and discard evidence about indicia of internal mental states. The fact that parties submit their cryptographic private keys to commit their resources to the smart contract is proof of such an intent.

The parties' mutual intent to be bound does not, however, prove a meeting of the minds about the specific contractual provisions. The doctrine of mutual mistake excuses performance when both parties were mistaken about an essential fact.[234] If the smart contract refers to cotton delivered by the ship *Peerless* but there are two—or

---

231. *See, e.g.*, Cohn v. Fisher, 287 A.2d 222, 224 (N.J. Super. Ct. Law Div. 1972) ("The essentials of a valid contract are: mutual assent, consideration, legality of object, capacity of the parties and formality of memorialization."); RESTATEMENT (SECOND) OF CONTRACTS §§ 12, 17, 71, 178–79 (AM. LAW INST. 1981).

232. In all the cases below, it may be possible to write exceptions into the smart contract, or into the basic code of the underlying blockchain platform, to address these situations. *See infra* Part IV.C.1. Such mechanisms are likely to be imperfect, however, and will compromise the efficiency of fully automated smart contracts. They will not automatically apply to every smart contract like a common law doctrine or statutory provision in conventional contract law.

233. *See supra* note 134 and accompanying text.

234. *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 20(1) & illus. 2, 152 (AM. LAW INST. 1981).

seventeen—ships of that name, standard contract law can hold the agreement unenforceable.[235] But the smart contract would go ahead and execute.[236] In a unilateral contract, the mistake might not even need to be mutual for a court to rescind it.[237] In other words, there might be an executable smart contract that does not satisfy the legal conditions for mutual assent. This is because even seemingly ex ante elements of contract law, like assent, actually turn on how matters look ex post.

The basic problem here is that smart contracts are not really smart, at least not in the way that contract law is smart. Smart contracts are not smart enough to adjust as events unfold. Even beyond mistakes, parties may not anticipate the exact scenario that arises at the time of performance. Most contracts are incomplete, in the sense that they do not specify an outcome for every possible state of the world.[238] Courts can fill in the blanks when the contractual expression of the parties' intent is unclear. With a smart contract, this approach is foreclosed.

A second problem related to meeting of the minds arises when the contract itself is clear, but does not represent the intent of the parties, for example, if a party enters into an agreement due to fraud or duress. In such a situation, performance may be excused.[239] The contract itself is valid; it is simply not enforceable. Yet, the distinction between validity and enforceability is precisely the one that smart contracts elide.

A smart contract is valid if it is accepted as part of the consensus process on the blockchain ledger. Once that happens, it is ineluctably enforced, even if fraudulently induced. The blockchain does not have

---

235.   *See* Raffles v. Wichelhaus, 159 Eng. Rep. 375, 376 (Ex. 1864). For the fact that there were at least eleven ships called *Peerless*; *see* A. W. Brian Simpson, *Contracts for Cotton to Arrive: The Case of the Two Ships Peerless*, 11 CARDOZO L. REV. 287, 295 (1989).

236.   Probably the smart contract would use whichever *Peerless* arrived first. If a multisig arbitration arrangement were built into the smart contract, the arbitrator could choose one option. However, the arbitrator would not have the ability, absent a specific contractual provision, to return the funds to both parties and recreate the ex ante status quo.

237.   *See, e.g.*, Conduit & Found. Corp. v. Atlantic City, 64 A.2d 382, 385 (N.J. Super. Ct. Ch. Div. 1949) ("Quite plainly, this is a unilateral mistake in a contract for which equity may, under certain circumstances, grant relief by way of rescission."); Chicago, St. Paul, Minneapolis & Omaha R.R. v. Washburn Land Co., 161 N.W. 358, 361 (Wis. 1917) ("[E]quity will grant relief by rescission in proper cases for the mistake of one party as readily as for mutual mistake, where it is shown that it would be contrary to equity and against conscience to allow the enforcement of the contract.").

238.   *See* Oliver D. Hart, *Incomplete Contracts and the Theory of the Firm*, 4 J.L. ECON. & ORG. 119, 123 (1998).

239.   *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 162, 175 (AM. LAW INST. 1981).

any context regarding *why* parties provide private keys to authorize a smart contract, only that they did. And no one can ask an arbiter to excuse performance because she signed with a gun to her head, because there is no arbiter. The arbiters are the computers operating the blockchain, and they only listen to the code of the smart contracts themselves.

As a practical matter, furthermore, the plaintiff in such a scenario would have difficulty asserting an affirmative cause of action. Duress itself is not a tort. And fraud is significantly different as a cause of action than as an affirmative defense.[240] The most effective recourse for someone improperly induced to enter in a smart contract would likely be to sue for restitution of the ill-gotten gains, after the smart contract executes.

2. *Problems with Consideration.* Similar problems arise with consideration, another basic requirement for an enforceable contract. Consideration distinguishes contracts from unenforceable gifts.[241] All promises may create moral duties, but not all promises create legal obligations. For smart contracts, there is no test for consideration. A typical smart contract involves some consideration that induces the reciprocal promise. However, there is nothing stopping someone from encoding a gift promise to the blockchain. Such a promise would execute irrevocably, in the same manner as any other smart contract. The rest of consideration doctrine, like the distinction between adequacy and sufficiency, similarly goes by the wayside when there is no way to test enforceability before execution.[242]

The absence of consideration from smart contracts sheds further light on how they differ from legal contracts. Consideration doctrine supports the view that contract law exists to provide remedies for

---

240. *See* RESTATEMENT (SECOND) OF CONTRACTS ch. 7, topic 1, intro. note (AM. LAW INST. 1981) ("Because tort law imposes liability in damages for misrepresentation . . . the requirements imposed by contract law are in some instances less stringent. Notably, under tort law a misrepresentation does not give rise to liability for fraudulent misrepresentation unless it is both fraudulent and material, while under contract law a misrepresentation may make a contract voidable if it is either.").

241. *See* JOSEPH M. PERILLO & JOHN D. CALAMARI, CALAMARI AND PERILLO ON CONTRACTS § 4.1 (6th ed. 2009); Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 815 (1941).

242. As another example, the preexisting duty rule in contract law rejects modifications which lack independent consideration. *See* Lingenfelder v. Wainwright Brewery Co., 15 S.W. 844, 848 (1891); RESTATEMENT (SECOND) OF CONTRACTS § 73 (AM LAW INST. 1981). If a smart contract does specify the opportunity for mutual modification, it need not incorporate a consideration requirement when doing so.

breach, and not to generate ex ante obligations.[243] If the point of contract were to enforce promises, or to allow parties to advert to liability voluntarily, contract law ought to allow them to make binding gift promises. But from its ex post vantage point, contract law can distinguish unenforceable gifts and mutual legal obligations. By contrast, smart contracts load all the effort into the ex ante specification of contractual terms.

3. *Problems with Capacity*.   The issues with legal capacity are somewhat different. Here, the question is not what the contract includes, but who it binds. Those without legal capacity, including children, people with significant mental impairments, and the excessively intoxicated, are excused from contractual performance.[244] As with consideration, smart contracts have no means to test for capacity. There is no legal limitation on minors having private encryption keys or owning Bitcoins, as they are currently restricted from having credit cards or accounts on payment services like PayPal.[245] And if someone digitally signs a smart contract while dead drunk, or another person exploits those circumstances to get them that person do so, there is no future opportunity for subjective evaluation by the other party.

The absence of a capacity test raises a deeper set of issues for smart contracts. The parties to a smart contract, at a technical level, are not people. They are cryptographic private keys. The secret private key represents the individual, based on a mathematical relationship with the associated public key. It is virtually impossible for someone who does not possess the private key to generate a valid digital signature that matches a given public key. This allows cryptographic keys to form the basis for digital identity systems.[246] Identity, however, is a rich

---

243.   *See supra* Part III.C.

244.   *See* RESTATEMENT (SECOND) OF CONTRACTS § 12 (AM. LAW INST. 1981). As with meeting of the minds, this is an objective test. *See id.* § 12(1) ("Capacity to contract may be partial and its existence in respect of a particular transaction may depend upon the nature of the transaction or upon other circumstances.").

245.   *See* Sean Williams, *Americans' Average Credit Score Is Rising—How Does Yours Compare?*, NEWSWEEK (Dec. 4, 2016, 8:00 AM), http://www.newsweek.com/americans-average-credit-score-rising-527641 [https://perma.cc/3AVE-HBEU] (noting that the CARD Act of 2009 prohibited those under 21 from obtaining credit cards without a parent cosigning or evidence of sufficient income to pay debts); PAYPAL, USER AGREEMENT FOR PAYPAL SERVICES § 1.2, https://www.paypal.com/ga/webapps/mpp/ua/useragreement-full   [https://perma.cc/75M2-GGXN] ("To be eligible to use the PayPal Services, you must be at least 18 years old . . . .").

246.   *See* L. Jean Camp, *Digital Identity*, IEEE TECH. & SOC'Y, Fall 2004, at 34, 40.

concept, and requires layering various capabilities for authentication, access, and more.[247] Moreover, even if a key uniquely belongs to an individual, the person and the key are not the same. An individual may possess many digital identities, backed by different private keys. The key may be linked to personally identifiable information that points to the specific individual. On the other hand, the key may designate a persistent digital identity hiding the associated real-world person, "pseudonymity," or, it may give no information at all about identity, "anonymity."

It may not be right, then, to say that smart contracts are agreements between people. In the case of the computable or data-oriented contract, the negotiation and specification of an agreement may be left entirely to machines.[248] But there, it is generally easy to view the computers as agents for their human programmers, who specify the conditions under which the computers can contract. The relevant practical difficulties, are not so different from those which agency law has addressed for centuries. With a smart contract, however, the connection between the humans and the agreement becomes more attenuated. The power of execution and enforcement is given over entirely to machines. The humans no longer have the capacity, in the colloquial sense, to avoid performance of the agreement. Perhaps they likewise do not have the capacity, in the legal sense, to perform it.

This analysis connects with the conclusion above that smart contracts are not promises, even if they are contracts.[249] That may be easy to accept conceptually, but as the foregoing discussion shows, things start to unravel when viewed doctrinally. Law bakes in assumptions about the human nature of contract. It may not be difficult as a thought experiment to imagine a contract that does not meet contract law's doctrinal specifications. However, once one dives into the analytical problems of contract law, the difficulties quickly multiply. This illustrates why smart contracts could not supplant contract law.

4. *Problems with Legality*.   Perhaps tautologically, a legally enforceable contract cannot effectuate an illegal purpose. Smart contracts, however, are not enforced by the legal system. Imagine, for

---

247.   *See id.*

248.   *See supra* Part I.A.

249.   *See supra* Part II.A.

example, a price-fixing conspiracy implemented through a series of smart contracts that adjust prices in lockstep.[250] The participants could be prosecuted under antitrust law, but the smart contracts would continue to operate. Further, there is no mechanism to stop a smart contract from implementing an unconscionable term, or a term that incorporates liquidated damages amounting to a penalty. Because the smart contract is self-executing, an action in court finding the terms unenforceable may have no practical effect; the contract will be performed regardless.

The legality test and various public policy rules hint that contract, generally considered a bastion of private law, retains a penumbra of public law. Again, this reinforces the view that contract law is an adjudicative mechanism, and is not principally concerned with reasons and obligations.[251] Legal adjudication is a public function, drawing on the coercive power of the state. Individuals acting together may have no problem effectuating a scheme in derogation of public policy, but as Thomas Hobbes argued, the state is granted an extraordinary monopoly on violence for the very purpose of preventing the war of all against all.[252]

These arguments of political theorists imagining a hypothetical state of nature become tangible with smart contracts. The hacking of The DAO illustrated the problem with contracts that have no opportunity for public oversight.[253] The hack was simultaneously valid as an enforceable smart contract within the software system, yet demonstrably invalid as theft in the minds of the contracting parties. If the perpetrator had exploited a bug in a conventional crowdfunding service such as Kickstarter to siphon off investors' funds, there would be no practical or legal difficulty in canceling the suspect transactions and returning the funds. Ethereum, in contrast, had no alternative to the nuclear option of the hard fork. While that may have fixed the immediate problem, the solution used a bazooka to shoot a mouse and caused significant collateral damage.

Even if a hard fork is effective, it transfers final adjudication from the institution of the courts to the polity of validation nodes.[254] A hard

---

250. This scenario of an algorithmic conspiracy has in fact been suggested by competition law experts. *See* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION 47–52 (2016).

251. *See supra* Part III.

252. *See* HOBBES, *supra* note 6.

253. *See* Popper, *supra* note 172.

254. Even if a court wished to halt execution of a smart contract such as the one through which funds were stolen from The DAO, there would not necessarily be any party to enjoin. *See supra*

fork stands or falls on whether a majority of the mining power in the blockchain network adopts it. This is not how contracts work. We do not adjudicate disputes through opinion polls or the ballot box. We grant the judge or jury authority to decide, constrained by the procedures of the legal system, the traditions of the common law, and the opportunity for legislative modification going forward. The limitations of direct democracy are familiar to anyone who has read the *Federalist Papers*.[255] Miners' interests may be even further removed from those of the community as a whole than "factions" in a democracy.

This is not to say that smart contracts are a threat to democratic values. One can imagine many scenarios in a world where smart contracts are prevalent, but legal analysis cannot rest entirely on imagined scenarios. We have no way of knowing how popular smart contracts will become, let alone how frequently controversies like The DAO hack will arise. What matters is that the seemingly abstract conflicts between smart contracts and basic doctrines of contract law touch deeper nerves, with potentially significant consequences. And, as in Part III, we investigate smart contracts for what they illuminate about conventional contracts.

C. Looking Forward

Having established that smart contracts both clarify the purpose of contract law in theory and challenge its application in practice, we conclude with a sketch about what happens next. Any recommendations at this time are necessarily provisional. Smart contracts are so new, and their prospects are so uncertain, that firm predictions are unwise, let alone normative judgments from those predictions. However, that is no reason to ignore potential consequences while there is still time to avoid them. And given the various considerations we have discussed, it is unreasonable to assume smart contracts will be implemented seamlessly.

1. *Best Practices*. The parties entering into smart contracts are not powerless to avoid their shortcomings. Knowing they cannot rely on the judicial decisionmakers to fill gaps, one can expect parties to put more effort into contract design and drafting.[256] Additionally, just as

---

note 96 and accompanying text.

    255. *See, e.g.*, THE FEDERALIST NO. 10 (James Madison).

    256. *See* Karen Eggleston, Eric A. Posner & Richard Zeckhauser, *The Design and*

transactional lawyers provide expertise in the construction of business agreements, a new class of "legal engineers" may arise to aid in the creation of smart contracts.[257] Parties can also employ technical mechanisms to lessen the rigidity of smart contracts. For example, giving authority to human oracles who decide whether the factual basis for performance has been met,[258] or employing arbitrators who resolve disputes through a multisig arrangements,[259] may avoid some of the draconian implications of fully self-enforcing agreements.

Already, organizations involved in the development of smart contract platforms are starting to create templates that embody best practices for smart contract drafting.[260] Using these templates, parties could avoid repeating mistakes in prior smart contracts, and they could draw on the expertise of industry groups carefully thinking about potential pitfalls. Smart contracting systems or, "contractware" to use Raskin's term,[261] could be programmed to offer templates automatically based on the desired agreement. Default terms, for example, requiring an opportunity for mutual modification prior to execution, could be mandatory to issue a smart contract on a particular platform. Parties could consult technical auditing firms to certify the integrity of smart contract code.[262] Even if the platforms are not subject to any legal duties regarding the contracts they enable, they still may care about avoiding harmful outcomes due to either ignorance or malfeasance by parties.

We cannot predict how well this optimistic story will play out. Surely, technical mechanisms for improving the quality of smart

---

Interpretation of Contracts: Why Complexity Matters, 95 NW. U. L. REV. 91, 120 (2000) (making a similar point about parties entering into incomplete contracts with uncertainty about enforcement).

257.   *See* Nina Kilbride, *Blockchain Legal Engineering*, MONAX BLOG (May 2, 2016), https://monax.io/2016/05/02/blockchain-legal-engineering/ [https://perma.cc/5RUG-VCV7].

258.   *See supra* note 118.

259.   *See supra* note 152.

260.   *See* CHRISTOPHER D. CLACK, VIRAM A. BAKSHI & LEE BRAINE, BARCLAYS BANK PLC, SMART CONTRACT TEMPLATES: FOUNDATIONS, DESIGN LANDSCAPE AND RESEARCH DIRECTIONS (Aug. 4, 2016), https://arxiv.org/pdf/1608.00771v2.pdf [https://perma.cc/6FZR-NGPW]; Ian Allison, *Barclays' Smart Contract Templates Stars in First Ever Public Demo of R3's Corda Platform*, INT'L. BUS. TIMES (Apr. 18, 2016 3:45 PM), http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329 [https://perma.cc/8JHG-45BY].

261.   *See* Raskin, *supra* note 23, at 307.

262.   Such smart contract code auditing firms are already beginning to spring up. *See, e.g.*, *About*, ZEPPELIN SOLUTIONS (2017), https://zeppelin.solutions/about [https://perma.cc/85BK-Z7RJ].

contracts will not eliminate the potential problems, any more than the ready availability of skilled lawyers prevents disputes over legal contracts.

2. *Restitution.* It would be a grave mistake to think that smart contracts will eliminate litigation. Litigation—like nature—will find a way. Parties will inevitably feel they were treated unfairly at times, and they will inevitably bring those complaints to court. The difference, however, will be the posture of the litigation. Rather than complaining parties seeking fulfillment of alleged promissory obligations, complaining parties will seek to undo or reverse completed transactions. Litigation will persist, but it will shift from claims of breach, to claims of restitution.

One might think that this effectively shifts contracts from liability rules to property rules.[263] That's not quite right, because one could have a smart contract that awards liability damages in a self-executing way. Rather, the difference is between ex ante enforcement and ex post adjudication. We have tried to illustrate that it is a mistake to conceive of these as simply two different forms of "enforcement."[264]

An effort to recover already-transferred resources is different than an effort to enforce an agreement. Thus, an action for restitution is very different than an action for breach of contract. At a minimum, the roles of the parties are reversed. In an action for breach, the nonperforming party seeks to enforce a transaction; whereas, in an action for restitution, the performing party seeks to reverse the transaction. Reversing who stands as plaintiff shifts the burdens of proof and litigation. In situations such as mutual mistake, there may be no a priori reason to favor one side. But when actions arise from claims of fraud, repugnance to public policy, or gifts without consideration, the balance of equities may shift in undesirable ways.

Those seeking redress for injuries suffered due to smart contracts may be forced to plead actions beyond quasi contract. To take an example highlighted earlier, both the plaintiff and the defendant can raise a claim of fraud, but the legal context is quite different. The plaintiff's claim is a tort, the defendant's claim is an affirmative defense in contract, and the legal requirements are different. Moreover, in

---

263. *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089, 1106–10 (1972) (distinguishing property and liability rules).

264. *See supra* Part III.

practice, such litigation may unfold quite differently if the focus shifts from the contract to the technical structures associated with it.[265] Because the transfer of value associated with the smart contract is tied to the parties' cryptographic private keys, the plaintiff may need to sue to force the defendant to give up that key, or perhaps computer passwords protecting it. Law enforcement agencies have done just that, when pursuing proprietors of Bitcoin exchanges promoting illegal activity like drug trafficking.[266] If that is the model, however, we have strayed quite far from the private law domain of contract.

3. *Regulation.* Indeed, the paradoxical result of smart contracts may be to expand the scope of government intervention into technological advancements, which has traditionally been a paradigmatic environment of private ordering. Once again, the shift from ex post adjudication to ex ante enforcement creates an inversion. Contracts free individuals to trust each others' commitments because they can rely on the power of the state to enforce them in cases of breach. Smart contracts remove the state from adjudication, but in so doing, they create pressure to reintroduce the state at the front end of the process. The only way to prevent smart contracts from facilitating illegal or disfavored conduct is to regulate them.[267]

It is a myth that the blockchain is inherently incompatible with regulation.[268] Any distributed ledger system may be more or less

---

265. By analogy, the development of autonomous vehicles has given new life to the philosophical Trolley Problem and raised the question of how one can sue a car for injuries caused by its algorithms. *See* John Markoff, *Should Your Driverless Car Hit a Pedestrian to Save Your Life?*, N.Y. TIMES (June 23, 2016), https://www.nytimes.com/2016/06/24/technology/should-your-driverless-car-hit-a-pedestrian-to-save-your-life.html [https://perma.cc/C5DZ-26NG] (relating autonomous vehicles to the classic Trolley Problem); Matt McFarland, *Who's Responsible When an Autonomous Car Crashes?*, CNN TECH (July 7, 2016), http://money.cnn.com/2016/07/07/technology/tesla-liability-risk/ [https://perma.cc/8DLM-ELXS]. Uber required passengers of its autonomous vehicle pilot program in Pittsburgh to agree to terms of service waiving any right to sue for injuries. *See* Mark Harris, *Passengers in Uber's Self-Driving Cars Waived Right to Sue for Injury or Death,* GUARDIAN (Sept. 26, 2016), https://www.theguardian.com/technology/2016/sep/26/uber-self-driving-passengers-pittsburgh-injury-death-waiver [https://perma.cc/85DX-XSY9]. Whether this waiver is enforceable is another question.

266. *See* Jon Matonis, *Key Disclosure Laws Can Be Used to Confiscate Bitcoin Assets*, FORBES (Sept. 12, 2012, 9:50 AM), https://www.forbes.com/sites/jonmatonis/2012/09/12/key-disclosure-laws-can-be-used-to-confiscate-bitcoin-assets/#4e414655ef54 [https://perma.cc/3JS9-L9GE].

267. *See* Raskin, *supra* note 23, at 340; *cf.* Scholz, *supra* note 33 (making similar arguments for regulation of algorithmic contracts).

268. *See* Jerry Brito, *Foreword* to PAUL ANNING ET AL., THE LAW OF BITCOIN, at xiii, xiii (Stuart Hoegner ed., 2015) ("A common misconception about Bitcoin is that it is not regulated."); Jerry Brito, *Bitcoin Remains a Tool for Freedom, Even While Going Mainstream*, REASON.COM

decentralized, and more or less anonymous, based on its technical design. Bitcoin and Ethereum are examples of "permissionless" systems that have no supervisory entity authorized to accept or reject participation in the mining network.[269] Other smart contract platforms, such as the Corda system for interbank transactions, only recognize trusted nodes, such as member banks.[270] This makes them less resistant to government intervention or private domination. A Corda smart contract could easily be subject to regulatory oversight, like the Anti-Money Laundering and Know Your Customer regulations that mandate identification of bank customers.[271] Even for a permissionless system, centralized intervention is not impossible; it is just very difficult and costly, as shown by the Ethereum hard fork to resolve The DAO hack.[272]

Perhaps a more apt parallel is the regulation of digital signatures. With the rise of e-commerce in the 1990s, it quickly became clear that digital signatures based on public-key cryptography could solidify commitments in the same manner as conventional signatures on traditional contracts.[273] A digital signature, however, is not really a

(May 19, 2014), http://reason.com/archives/2014/05/19/bitcoin-remains-a-tool-for-freedom-even [https://perma.cc/AAW8-6FCR] ("The cold logic of economies of scale tend to lead to greater centralization, and thus more regulation, and this will likely happen to Bitcoin, too."); Wright & de Filippi, *supra* note 22, at 4 ("[T]here will be an increasing need to focus on how to regulate [blockchain technology]."). *But see* Ariel Deschapell, *Why Regulating Bitcoin Won't Work*, COINDESK (Feb. 25, 2014, 14:00) http://www.coindesk.com/why-regulating-bitcoin-will-not-work [https://perma.cc/BM4R-BXEW] ("This is what scares governments, but the point they seem to miss, is that for better or worse, they can't do anything about [regulating Bitcoin]."). *See generally* Werbach, *supra* note 17 (arguing that in fact, legal harmonization and regulation are essential to fulfilling the promise of the blockchain).

269. *See* Swanson, *supra* note 99 (explaining the distinction between permissioned and permissionless blockchains).

270. *See id.*; Michael del Castillo, *R3 Announces New Distribution Ledger Technology Corda*, COINDESK (Apr. 5, 2016, 10:34 PM), http://www.coindesk.com/r3cev-blockchain-regulated-businesses/ [https://perma.cc/4L4Z-2M2U].

271. *See* Ian Allison, *R3 Develops Proof-of-Concept for Shared KYC Service with 10 Global Banks*, INT'L. BUS. TIMES (Nov. 10, 2016, 4:15 PM), http://www.ibtimes.co.uk/r3-develops-proof-concept-shared-kyc-service-10-global-banks-1590908 [https://perma.cc/7AM7-7TPP]; Aleya Begum, *R3's Corda Uncovered: It's Not Blockchain*, GLOBAL TRADE REV. (Oct. 1, 2017), http://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-uncovered-not-blockchain [https://perma.cc/LZ7K-HMZ9] ("Corda takes a different approach. By default, information about transactions is only shared with those parties to a transaction.").

272. *See supra* note 173 and accompanying text.

273. *See* Tim Squitieri & Paul Davidson, *E-Signatures Seen as Big Boon to Business: Companies Expect to See Huge Savings*, USA TODAY, June 15, 2000, at 7A; John Schwartz, *E-Signatures Become Valid for Business*, N.Y. TIMES (Oct. 2, 2000), http://www.nytimes.com/2000/10/02/business/e-signatures-become-valid-for-business.html [https://perma.cc/J5YK-7XDM].

signature at all. It is a private key that generates an associated public key. Ultimately, the E-SIGN Act preempted contrary state law, and ensured that rules requiring signatures could be satisfied with their digital analogues.[274] The legal effects and limitations of digital signatures were therefore not defined by handwriting specialists, but by government.

Under many scenarios, regulators might interpose themselves into the workings of smart contracts. Generally speaking, these will involve regulation of the contracting software platforms or blockchain validation nodes, rather than the parties themselves. Someone knowingly entering into an illegal smart contract has still violated the law, but it will likely be easier to police the enabling systems.[275] The kinds of smart contracts parties can form will depend on the functionality and interfaces of the available tools. This recalls the fate of P2P file-sharing systems like Napster, which facilitated widespread copyright infringement. The Supreme Court eventually concluded that even when P2P services had no specific knowledge of or ability to prevent infringing transfers, the services were still liable if set up to induce them.[276] A smart contract system that facilitated copyright infringement, for example, by granting users digital rights to content without proper licenses, would likely suffer the same fate.

As noted earlier, nothing technically prevents execution of an illegal smart contract.[277] The infamous Silk Road online marketplace used Bitcoin payments to facilitate sales of illegal goods, but the transactions themselves used the same electronic contracting mechanisms as legitimate sites like Amazon.com or Ebay.[278] If smart contracts can further automate such activities, or financial crimes like money laundering, there will be pressure to prohibit intermediaries from enabling or processing them. Moreover, legal requirements, like the automatic stay in bankruptcy law, can supersede contractual obligations. Courts and legislatures may attempt to require smart

---

274. Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, § 101.114 Stat. 464 (2000) (codified at 15 U.S.C. § 7001 (2012)); *see also* Jay M. Zitter, Annotation, *Construction and Application of Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C.A. §§ 7001 to 7006*, 29 A.L.R. Fed. 2d 519 (2008) (explaining that a signature may not be denied solely because it is electronic, but that acceptance of electronic signatures are not mandatory).

275. *See* Raskin, *supra* note 23, at 340 (suggesting that illegal smart contracts be subject to regulation).

276. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 936–37 (2005).

277. *See supra* Part IV.B.4.

278. *See supra* note 100.

contracting systems to incorporate exceptions for such contexts.[279]

Administrative regulation of smart contracts is also a possibility. Various agencies, including the Federal Trade Commission (FTC), the Securities and Exchange Commission, and the Consumer Financial Protection Board, have authority to prevent unfair or deceptive practices. This extends to situations where companies do not intend consumer harms, but fail to take sufficient precautions against them. For example, the FTC successfully brought an enforcement action against Wyndham Hotels for inadequate information security practices, which led to losses of customer data.[280] One could imagine a similar action against the developers of The DAO, the Ethereum Foundation, or miners who processes its transactions, based on their failure to offer adequate safeguards for funds pledged to the crowdfunding system.[281] It is difficult to evaluate what this would mean in practice. The Ethereum Foundation is a Swiss nonprofit, The DAO software is an open-source project, and the miners are a changing collection of voluntary participants around the world. Imposing regulatory obligations on any of them would be problematic. Yet if significant consumer harms materialize, regulators are unlikely to walk away.

An analogous situation occurred in the early days of the commercial internet. The Digital Millennium Copyright Act of 1998[282] gave intermediaries immunity from liability for copyright infringement, but only if they complied with notice-and-takedown procedures when notified of infringing material.[283] Congress or a state legislature concerned about smart contracts running amok might grant a safe harbor to software creators, application providers, and validation node operators, but condition that safe harbor on the adoption of templates, functional limitations, and audits for executable smart contracts. Such rules could be vague or overbroad, chilling the adoption of smart contracts, or they might provide security for parties who otherwise would be disinclined to use smart contracts. At this point, the specifics are too difficult to predict with any confidence.

---

279. *See* Raskin, *supra* note 23, at 327–29.

280. *See* F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 615 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (upholding the FTC's action).

281. One way to reach these parties would be to treat the smart contracts as legal agents of their creators. *See* Scholz, *supra* note 33.

282. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified at scattered sections of 17 and 28 U.S.C.).

283. 17 U.S.C. § 512 (2012).

To some degree, this is a familiar story. Where freedom of contract stands in the way of important public policy objectives, it must give ground. That occurred most famously when the New Deal eventually broke through the *Lochner* Court's resistance to economic regulation.[284] Smart contracting systems offer a kind of technical due process protection from legislative or judicial interference. While they may hold the state at bay to an extent, they will not eliminate it from the picture.

CONCLUSION

Our goal has been to analyze smart contracts from the perspective of law—and vice versa. Though there is significant evidence smart contracts will eventually enjoy widespread adoption, we make no assumptions about their technical and business trajectory. Even if smart contracts turn out to be a fad, they can help us better understand legal contracts. And if blockchain-based smart contracts fail, another technology will inevitably arise to achieve the same objectives. The very act of unpacking smart contracts may help to anticipate—and thus, to mitigate—potential difficulties.

Smart contracts are just one part of the larger trend of computerized technologies purporting to displace or replace human decisionmaking.[285] In areas like hiring, finance, and copyright enforcement, algorithmic systems are touted for their speed, efficiency, and reliability, unlike error-prone and potentially biased humans. Indeed, the benefits are considerable. But it quickly becomes clear that machines are prone to their own errors and biases.[286] Additionally, the introduction of algorithmic systems into historically judgment-laden fields creates challenges for legal and practical accountability.[287] As a

---

284. *See, e.g.*, Nebbia v. New York, 291 U.S. 502, 523 (1934) (upholding government price regulation on the grounds that "neither property rights nor contract rights are absolute; for government cannot exist if the citizen may at will use his property to the detriment of his fellows, or exercise his freedom of contract to work them harm").

285. *See generally* ANDREW MCAFEE & ERIK BRYNJOLFSSON, RACE AGAINST THE MACHINE (2011) (detailing the replacement of workers by computers).

286. *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015) (arguing that powerful economic actors use "black box" computer algorithms to expand their power, often unfairly); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016) (describing how machine learning algorithms can produce discriminatory outcomes).

287. *See generally* PASQUALE, *supra* note 286; Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, 19 STAN. TECH. L. REV. 473 (2016) (examining the difficulties of enforcing copyrights through online intermediaries and proposing a

result, both legal scholars and computer scientists are developing techniques to promote fairness and transparency in these decisions.[288] A similar dynamic can be expected for smart contracts.

Contract law is nothing if not resilient. We have little doubt it will survive the onslaught from smart contracts, if indeed that is what is happening. However, contract law may learn something about itself from its new challenger.

---

new accountability framework).

288. *See* Barocas & Selbst, *supra* note 286, at 675; Nicholas Diakopoulos, *Accountability in Algorithmic Decision Making*, 59 COMM. OF THE ACM 56, 62 (2016); Joshua A. Kroll et al., *Accountable Algorithms,* 165 U. PA. L. REV. 633, 637–38 (2017); Michael Feldman et al., *Certifying and Removing Disparate Impact*, *in* 21 PROC. ACM SIGKDD CONF. ON KNOWLEDGE DISCOVERY & DATA MINING 259 *passim* (2015), https://ww3.haverford.edu/computerscience/faculty/sorelle/papers/kdd_disparate_impact.pdf [https://perma.cc/7GSG-5BAJ].