CONTRACTS *EX MACHINA*

Kevin Werbach* and Nicolas Cornell**

67 Duke Law Journal __ (forthcoming)

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: Can smart contracts offer a superior solution to the problem 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 can illuminate the role of contract law more than they can obviate it.

Technological advancements hold the potential to alter our very conception of the law. It has already become commonplace to suggest that technologies can operate as a kind of law, regulating behavior of their users.[1] But, thus far, traditional legal enforcement has generally remained available as a backstop. Is it possible for emerging technologies to

* Associate Professor, Legal Studies and Business Ethics Department, The Wharton School, University of Pennsylvania.

** Assistant Professor, Legal Studies and Business Ethics Department, The Wharton School, University of Pennsylvania.

[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* Bruno Latour, *On Technical Mediation*, 3.2 COMMON KNOWLEDGE 29 (1994); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012).

displace the law even for enforcement—in what might be considered law's historically essential province? In this article, we examine a potentially significant contemporary example: digitally enforced "smart contracts" based on the distributed cryptocurrency technology of Bitcoin and the blockchain.[2] Enthusiasts of various stripes believe that smart contracts offer the potential to displace the legal system's core function of enforcing agreements.

It has long been thought 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.[3]

Hobbes's basic idea—that binding agreements require a system to ensure that counterparties can trust one another to perform—is an intuitive and powerful argument for the essential role of the law.[4]

And yet recent technological advances have led to speculation that the apparatus of contract law might soon be largely or entirely displaced.[5] One commentator succinctly

---

[2] The term "smart contracts" was coined by cryptographer Nick Szabo in the 1990s. *See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997), http://ojphi.org/ojs/index.php/fm/article/view/548.

[3] THOMAS HOBBES, LEVIATHON, ch. XIV, para. 18-19 (1st ed. n.p. 1651). *See also* 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).

[4] *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.").

puts this radical claim as follows: "Smart 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."[6] 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."[7] Even world leaders have taken notice, with Russian Prime Minister Dmitry Medvedev declaring "Smart Contracts represent [a] new challenge to legal regulation. Systems creating such contracts live by their own rules, beyond the boundaries of law."[8] In short, smart contracts are believed to 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 will obviate the need for contract law, revolutionize business arrangements, and restructure property ownership.[9] Skeptics see the blockchain foundation as little more than a Ponzi scheme.[10] Some technologists argue

---

[5] *See, e.g.*, Matt Byrne, *Do lawyers have a future?*, THE LAWYER, Sept. 20, 2016 ("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.").

[6] Alexander Savelyev, *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885241; *see also* DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION (2016) at 47 ("Smart contracts are unprecedented methods of ensuring contractual compliance, including social contracts."); Rob Marvin, *Blockchain in 2017: The Year of Smart Contracts*, PC MAG, Dec. 12, 2016, http://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts (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")

[7] Andrew Hinkes, *Blockchains, Smart Contracts, and the Death of Specific Performance*, INSIDE COUNSEL, July 2014; *see also* Matt Byrne, *Do Lawyers Have a Future?*, THE LAWYER, Sept. 20, 2016.

[8] Vystupleniye Dmitriya Medvedeva na plenarnom zasedanii [Speech of Dmitry Medvedev on Plenary Session], Saint Petersburg International Legal Forum, 18 May 2016, *quoted in* Savelyev, *supra* note 5.

[9] *See, e.g.*, *Not-So-Clever Contracts*, ECONOMIST, July 30, 2016 ("Such 'smart contracts' are all the rage among futurist backers of the blockchain, the technology that underpins bitcoin, a digital currency."); Arvind Narayanan, et al, Bitcoin and Cryptocurrency Technologies 2 (Princeton University Press 2016) (Feb. 9, 2016 draft) ("Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world."); NORTON ROSE FULBRIGHT, CAN SMART CONTRACTS BE LEGALLY BINDING CONTRACTS? (November 2016), http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts, at 2 (quoting R3 consortium CEO David Rutter stating that "smart contracts…will set the scene for the next twenty years of finance.").

[10] *See* Eric Posner, *Fool's Gold*, SLATE, April 11, 2013, at http://www.slate.com/articles/news_and_politics/view_from_chicago/2013/04/bitcoin_is_a_po

that, despite the name, smart contracts have nothing to do with contracts.[11] Yet one group conspicuously absent from the debate over smart contracts has been contract law scholars.

Upon inspection, the story is more complex than it seems. 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 a spectrum of electronic agreements that has been evolving over several decades. Firms can achieve significant cost savings and efficiency gains when using computers to automate contracting. Smart contracts could greatly extend those benefits, taking advantage of Bitcoin and the blockchain as open platforms for secure exchange of value without mutual trust.[12] As they are adopted, smart contracts will force courts, legislatures, and other legal actors to confront difficult questions about the application of basic contract doctrines. They may even be used in lieu of traditional contracting in some situations.

They will not, however, replace contract law. While smart contracts can meet the doctrinal requirements of contract law,[13] 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*.[14] Smart contracts bring into sharper relief this core function of contract law. They eliminate the act of remediation, by admitting no possibility of breach. The needs that gave rise to contract law do not, however, disappear. If the parties do not—or cannot—represent *ex ante* all possible outcomes of the smart

---

nzi_scheme_the_internet_currency_will_collapse.html; Matt O'Brien, *Bitcoin isn't the future of money — it's either a Ponzi scheme or a pyramid scheme*, WASHINGTON POST WONKBLOG, June 8, 2015, at 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/; Ferdinando Ametrano, *Why 2017 Will Prove Blockchain Was a Bad Idea,* COINDESK, Jan. 4, 2017, at http://www.coindesk.com/2017-will-prove-blockchain-bad-idea/ ("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.").

[11] *See, e.g.*, Monax, Explainer: Smart Contracts, https://monax.io/explainers/smart_contracts/ ("To begin with, smart contracts are neither particularly smart nor are they, strictly speaking, contracts.").

[12] *See* Kevin Werbach, *Law and Ledgers: The Blockchain and the Rebooting of Trust* (forthcoming)

[13] *See* Part II.A. *infra*.

[14] *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.").

contract arrangement, 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 only shift their complexion. In such scenarios, either the parties or the state will be driven to seek to reintroduce the machinery of contractual adjudication. Once one properly appreciates what is—and is not—the function of contract law, it becomes evident that reports of its death are "greatly exaggerated."[15]

The remainder of this Article unfolds as follows. In Part I, we describe the history and operation of smart contracts. In Part II, we analytically evaluate smart contracts, which have been under-theorized so far, asking how existing legal categories might or might not apply to smart contracts. In Part III, we consider whether smart contracts can, in fact, serve as a substitute for contract law. By answering this in the negative, we address 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.

I. CONTRACTS GET SMART

Smart contracts represent the fusion of two lines of technological development: electronic contracting and cryptography. They were first theorized and named two decades ago. However, significant interest in, and implementation of, smart contracts has occurred only recently. Viewed one way, smart contracts represent merely the latest step the evolution of electronic agreements. From another perspective, smart contracts' use of blockchain technology distinguishes them from any antecedents.

The cryptographer Nick Szabo, who coined the term, defined a smart contract as, "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[16] By using "a set of promises," Szabo left open whether a

---

[15] Though now part of popular culture, the familiar Mark Twain turn of phrase 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); *see also* Mark Twain, *Chapters from My Autobiography*, THE NORTH AMERICAN REVIEW, 21 Sept. 1906, p.160 ("I said, 'Say the report is greatly exaggerated.'").

[16] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996), http://szabo.best.vwh.net/smart_contracts_2.html. Max Raskin uses a simpler definition: "an agreement whose execution is automated." Max Raskin, *The Law of Smart Contracts*, GEORGETOWN TECH. REV. (forthcoming), *available at*

smart contract was enforceable as a legal contract."[17] We consider this question below.[18] His reference to protocols "with which" parties perform is similarly coy. Smart contracts do not just specify protocols for performance; they actually implement them. Szabo's definition has not been universally adopted, and subsequent authors offer subtly varied descriptions of the term. For purposes of this paper, we will use the following: A smart contract is an agreement in digital form that is self-executing and self-enforcing.[19]

In this Part, we examine the history and workings of smart contracts.

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 make arrangement through online ticketing systems rather than going to a travel agent, to give just a handful of examples. This automation process has already 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 performed automatically in limited circumstances, are nothing new.[20] For several decades, larger corporations have used electronic data interchange (EDI) formats to communicate digitally across supply chains.[21] The internet brought electronic commerce to ordinary

---

https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2842258, at 2. *See also* Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK (June 4, 2016, 18:39 GMT), http://www.coindesk.com/making-sense-smart-contracts (2016) ("Many debates about the nature of smart contracts are really just contests between competing terminology.").

[17] Others 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* Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (2015), at 10-11.

[18] *See* Part II.A. *infra*.

[19] In addition to enforcement, smart contract technologies could support the full range of pre-contractual and post-contractual activity. We explain the centrality of enforcement to smart contracts below.

[20] *See* Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012).

[21] 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

consumers. The average consumer today accedes to a digital contract every time they begin a relationship with an online service provider, merely by clicking a button.[22] These electronic contracts, however, are simply written agreements in digital costume. The contract is electronic merely 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 sees a document in English (or another language) spelling 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 is acceptance, because most consumers barely realize the existence of, let alone read, the contractual text. Courts had little difficulty disposing of this objection.[23]

The step beyond an electronic contract is what Harry Surden labels a "data-oriented" contract. This is a contact, "in which the parties have expressed one or more terms or conditions of their agreement in a manner designed to be processable by a computer system."[24] The distinction here is that that primary audience for the contract is a machine rather than a human.[25] For example, a financial option contract may grant the right to purchase a stock at a given price, expiring on a certain date. A data-oriented contract would represent that arrangement precisely 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. It gives the computer systems implementing a data-oriented contract the power "to make automated, *prima-facie* assessments about compliance or performance…."[26] In the option contract example above, the brokerage house computer system could evaluate itself whether the price and timing of a proposed purchase meet the terms of the option. The requirements for a

---

language. *See* JANE K. WINN & BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 5-59 (2001) (describing EDI); Surden, *supra* note 20, at n.30.

[22] *See* Brett M. Frischmann & Evan Selinger, Engineering Humans with Contracts, https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2834011.

[23] *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Hill v. Gateway 2000, Inc., 105 F.3d 1147 (7th Cir. 1997) (cert. denied, 522 U.S. 808 (1997)). 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 (2d Cir. 2002).

[24] Surden, *supra* note 20, at 639.

[25] 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.").

[26] *See id.* at 636.

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 as an input to that computation is available in digital form.[27] Giving machines the ability to determine whether a contract has been performed can dramatically reduce transaction costs.[28] Although there are significant challenges in accurately representing and interpreting contractual semantics computationally, computable contracts are being employed widely in fields such as finance.[29]

The evolution from electronic to data-oriented to computable contracts embodies a trend toward greater machine autonomy. Insofar as computers can increasingly take the place of humans in negotiating, forming, performing, and enforcing contracts, contracts can increasingly operate with the speed and consistency of machines.

The limitation of even computable contracts is that the computers involved can only make *prima facie* determinations about performance.[30] The legal system and other traditional mechanisms remain available to the parties if they are unsatisfied with the results of the automated systems.[31] The contract is designed to be computable, but if the computation diverges from the parties' actual intent (as conventionally understood in contract law), the computerized result is disregarded.[32] And even though computable

---

[27] *See id.* at 664.

[28] *See id*. at 689-95.

[29] *See id.*

[30] *See id*. at n.25.

[31] 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. However, they similarly fail to discuss the implications of implementing these formalized agreements as smart contracts. *See* Mark D. Flood & Oliver R. Goodenough, Contract as Automaton: The Computational Representation of Financial Agreements (March 26, 2015), *available at* http://ssrn.com/abstract=2538224. *See also* Cristian Prisacariu & Gerardo Schneider, *A Formal Language for Electronic Contracts*, *in* FORMAL METHODS FOR OPEN OBJECT-BASED DISTRIBUTED SYSTEMS 174–189 (Marcello M. Bonsangue & Einar Broch Johnsen eds., 2007), http://dx.doi.org/10.1007/978-3-540-72952-5_11 (proposing a formal language for writing electronic contracts).

[32] 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/ (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.

contracts can enable machines to contract automatically with one another, such autonomous operation is still relatively limited.[33]

In 1996-97, cryptographer Nick Szabo published a series of articles and blog posts outlining the functions and technical requirements for what he labeled "smart contracts."[34] Szabo's starting point was that networked digital protocols "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."[35] He suggested that, "[t]he contractual phases of search, negotiation, commitment, performance, and adjudication…can be embedded in [] hardware and software…."[36] Many of those functions were already being implemented electronically at the time, or would be soon with the rise of e-commerce. 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.[37] The simple electronic mechanism of a vending machine performs two critical functions. First, it directly effectuates performance, by taking in money and dispending products. Second, it incorporates enough security to make the cost of breach (breaking into the machine) exceed the potential rewards.[38] For all practical purposes, the vending machine is the entirety of the contractual environment for its transactions. It is not limited to the *prima facie* decisions of Surden's computable contracts; its performance of the contact is effectively final.[39]

Szabo's vision—that forming and performing contracts could be fully automated—was ahead of its time. His work, and similar ideas by others, were recognized within the community of "cypherpunks" designing technical mechanisms to ensure security and

---

[33] *See* Surden, *supra* note 20, at 695.

[34] *See* Szabo, *supra* note 2; Szabo, *supra* note 16; Nick Szabo, THE IDEA OF SMART CONTRACTS (1997), http://szabo.best.vwh.net/smart_contracts_idea.html; Nicholas J. Szabo, Smart Contracts (Presentation), http://w-uh.com/download/WECSmartContracts.pdf.

[35] Szabo, *supra* note 2.

[36] *Id.*

[37] *See id.*

[38] *See id.*

[39] 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.

privacy without reliance on governments.[40] However, these ideas remained largely distinct from the commercial world of electronic commerce.

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.[41] Ever since it appeared in a mysterious 2008 post by the pseudonymous Satoshi Nakamoto,[42] 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.[43] Over 100,000 firms including major companies such as Microsoft, Dell Computer, Dish Network, Time Inc., and Overstock.com accept Bitcoin-denominated transactions,[44] and the nominal value of Bitcoins in circulation briefly exceeded $18 billion at the beginning of 2017.[45] Venture capitalists have funded scores of Bitcoin-based startups, investing over $1 billion so far.[46] Most of the world's largest financial services firms are exploring or implementing related technologies. Legal scholars are beginning to take notice as well.[47]

---

[40] *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; Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED (Nov. 23, 2011, 2:52pm), https://www.wired.com/2011/11/mf_bitcoin/.

[41] As described below, 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 paper, may be implemented on the Bitcoin blockchain or other blockchains.

[42] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), http://nakamotoinstitute.org/bitcoin/. The identity of the person or persons who authored the paper remains unknown. *See* Popper, *supra* note 40.

[43] *See generally* NATHANIAL POPPER, DIGITAL GOLD (Harper, 2015) (surveying the burgeoning Bitcoin community).

[44] *See* State of Bitcoin 2015: Ecosystem Grows Despite Price Decline, COINDESK, http://www.coindesk.com/state-bitcoin-2015-ecosystem-grows-despite-price-decline/ (last visited July 5, 2015).

[45] *See* Market Capitalization, https://blockchain.info/charts/market-cap (last visited January 14, 2017).

[46] *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/

[47] *See* Wright & De Filippi, *supra* note 17; Joshua Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015); Raskin, *supra* note 16.

The core attribute of Bitcoin is that it allows unrelated individuals and organizations to have confidence in transactions even without trusting intermediaries or a legal system.[48] A currency requires trust because buyers and sellers must believe that the virtual tokens they exchange for assets of value will themselves have value. A $100 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.

Underlying Bitcoin is a technology called the blockchain, or more generally, distributed ledgers.[49] A distributed ledger allows any number of computers to keep an identical record of information, without having to reference a master copy.[50] This allows Bitcoin users to be confident that the same digital coin is not being spent multiple times, but that turns out to be just one use case. Developers and entrepreneurs are actively working on applying blockchain technology to applications including cloud file storage;[51] ridesharing;[52] name registration (as for the internet's Domain Name System);[53] crowdfunding;[54] device management for the Internet of Things;[55] online voting;[56]

---

[48] Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled Onto Something Much, Much Bigger*, BUSINESS INSIDER, April 22, 2014, http://www.businessinsider.com/the-future-of-the-blockchain-2014-4; Pete Rizzo, *VC Fred Wilson: Block Chain Could Be Bigger Opportunity than Bitcoin,* COINDESK, May 5, 2014

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

[50] *See* Hal Hodson, *Bitcoin Moves Beyond Mere Money*, NEW SCIENTIST, 2013, http://www.newscientist.com/article/dn24620-bitcoin-moves-beyond-mere-money.html#.VZmDmqa-uf4 (last visited Jul 5, 2015); *The Next Big Thing*, THE ECONOMIST, May 9, 2015, *at* http://www.economist.com/news/special-report/21650295-or-it-next-big-thing.

[51] http://storj.io/; http://maidsafe.net/.

[52] *See* Amanda Johnson, *La'Zooz: The Decentralized Proof-of-Movement "Uber" Unveiled*, COINTELEGRAPH (2014), http://cointelegraph.com/news/112758/lazooz-the-decentralized-proof-of-movement-uber-unveiled (last visited Jul 8, 2015).

[53] https://namecoin.info/.

[54] https://blocktrust.org; https://koinify.com/.

[55] *See* Paul Brody & Veena Pureswaran, DEVICE DEMOCRACY : SAVING THE FUTURE OF THE INTERNET OF THINGS (2015).

[56] *See* Danny Bradbury, *How Block Chain Technology Could Usher in Digital Democracy*, COINDESK (June 16, 2014, 23:05 GMT), http://www.coindesk.com/block-chain-technology-digital-democracy/.

verification of ownership and time-stamping for digital documents;[57] prediction markets;[58] and even establishing provenance of wine.[59]

There are three primary elements to the Bitcoin architecture: the blockchain, the network, and mining.[60] These three elements to combine to create a mechanism for ensuring trustworthiness without requiring trust in any particular institution or agent.

First, a blockchain is a shared public ledger of transactions.[61] This growing ledger incorporates an abbreviated reference (known as a cryptographic hash) of every approved transaction. A Bitcoin transaction is a cryptographically signed[62] statement on the blockchain transferring Bitcoin tokens between two or more accounts. These transactions are grouped together into blocks, with a new one appended approximately every ten minutes.[63] Anyone can view the Bitcoin blockchain, and trace back transactions all the way to the original "genesis block" created by Nakamoto.

The second element is the network. Bitcoin is a distributed system, so the blockchain is not stored in one central location. Instead, computers running the Bitcoin software connect in a peer-to-peer network, where each full participant[64] maintains a complete copy of the blockchain. Every transaction is broadcast across the network to all nodes,

---

[57] What is Proof of Existence?, http://www.proofofexistence.com/about.

[58] Jack Peterson & Joseph Krug, *Augur: a Decentralized, Open-Source Platform for Prediction Markets*, ARXIV PREPR. ARXIV150101042 (2015).

[59] The Future of Wine Provenance Is Bitcoin, VINFOLIO BLOG (2014), http://blog.vinfolio.com/2014/10/06/the-future-of-wine-provenance-is-bitcoin/ (last visited Jul 8, 2015).

[60] For a detailed but accessible technical description of Bitcoin, see Arvind Narayanan et al, Bitcoin and Cryptocurrency Technologies, *at* https://drive.google.com/uc?export=download&id=0B4-bDFu_72BeZnJRTTRRcHdibVk.

[61] *See* Fairfield, *supra* note 47.

[62] 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 blockchain. And therefore, unlike traditional financial transactions where the parties may not know identities but some intermediaries (such as banks) do, the actual identity of those transacting may be effectively impossible to determine.

[63] Some distributed ledger systems use data structures other than blockchains, but the basic architecture of the system is the same.

[64] *See* Narayanan et al, *supra* note 60.

which then add valid blocks to the blockchain on a regular basis. Individual consumers don't 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.[65]

The final element, mining, is perhaps the least intuitive aspect of Bitcoin. Yet it is perhaps the system's most significant innovation.[66] The reason decentralized trust systems are so difficult is that participants may be untrustworthy. Especially when there is a financial incentive to cheat or lie, some actors can be expected to do so. If there is any realistic possibility that malicious actors on the Bitcoin network could steal currency, or spend the same Bitcoins multiple times (effectively printing money),[67] 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 be honest. Bitcoin nodes repeatedly attempt to solve cryptographic 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.[68] The new block based on that solution is broadcast across the network. Other nodes, after checking for validity, add the new block to the blockchain.[69] The node that successfully proposed the new block receives a financial reward. The rewards for mining are what makes Bitcoin robust to attacks. Miners are incentivized to

---

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

[66] The more technical term for the mining process is Proof of Work.

[67] This is known as a double-spend transaction.

[68] The system is known as proof of work. *See* Adam Back, A Partial Hash Collision Based Postage Scheme, March 28, 1997, *at* http://www.hashcash.org/papers/announce.txt (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.

[69] 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 tradeoff is increased delay before they transfer the Bitcoins or associated assets.

apply as much computing power as possible to confirm valid blocks.[70] Malicious actors are effectively competing against the total computing power in the network.

An elegant aspect of Bitcoin's mining system is that the financial rewards take the form of Bitcoins themselves.[71] Because Bitcoin is accepted as a currency and can be exchanged for traditional currencies such as dollars, mining rewards are 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 added to the system. The mining reward is halved approximately every four years, meaning there will ultimately be no more than approximately 21 million Bitcoins ever created.[72] As an alternative compensation mechanism, Bitcoin allows parties to specify transaction rewards, which are deducted from the value of a validated transaction.[73] The expectation is that, as the block rewards decrease, voluntary transaction rewards will become the predominant incentive for Bitcoin miners.[74]

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.[75] An inherent constraint on traditional

---

[70] *Cf.* Kevin Werbach, BITCOIN IS GAMIFICATION (2014), https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22 (explaining the significance of the motivational system to Bitcoin).

[71] The block reward as of early 2017 is 12.5 Bitcoins, which equates to roughly $15,000 at current exchange rates.

[72] 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 designed as one Satoshi. So, even though the exchange rate of a Bitcoin is, as of early 2017, over $1,000, transactions can involve tiny amounts of money, far smaller than the equivalent of one cent.

[73] Nakamoto called these "transaction fees." *See* Nakamoto, *supra* note 42, at 4. We use "transaction rewards" to clarify that the sum if 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.

[74] *See id.* This premise remains untested.

[75] *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. SOCIOLOGICAL REV. 55

contracting is that the parties must trust the state, and often also a variety of private intermediaries that facilitate efficient operation of the system. Legal enforcement of contracts can be cumbersome and error-prone. Just as there are reasons to use a decentralized digital currency system even though traditional fiat currencies are extremely successful, decentralized digital contracts could analogously solve problems that the conventional contract system cannot. The basic challenge for such decentralized contracts is the same as for currencies: how to reliably ensure that commitments will be upheld and the participants will follow the rules.

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.[76] Bitcoin's success in decentralizing trusted financial transactions gives hope to those who advocate similar decentralization of trusted contractual agreements.[77] Smart contracts may actually be a bigger idea than Bitcoin as a currency.[78]

The critical distinction between smart contracts and other forms of electronic agreements is enforcement. A data-oriented or computable contract may be performed automatically by computers that determine the requisite state has been achieved. However, that execution can be interrupted at any point by humans. With a smart contract, complete execution of the agreement, including any transfer of value, occurs immutably.[79] The computers in the blockchain network ensure performance, rather than any appendage of the state.

(1963); *cf.* Carolina Camén, Patrik Gottfridsson, & Bo Rundh, *To Trust or Not to Trust?: Formal Contracts and the Building of Long-Term Relationships*, 49 MANAGEMENT DECISION 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.

[76] David Z. Morris, *Bitcoin is Not Just Digital Currency. It's Napster for Finance*, FORTUNE, 2014, http://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance/; Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST COMPANY CO.LABS, 2014, http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app.

[77] Nick Szabo, Forward, Smart Contracts: 12 Use Cases for Business & Beyond, at 3, http://digitalchamber.org/assets/Smart-contracts-12-use-cases-for-business-and-beyond.pdf ("Blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond.").

[78] *See* Cassano, *supra* note 76. 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 massive adoption of smart contracts.

[79] *See* Part II.B.3, *infra.*

The blockchain's distributed trust is what facilitates smart contracts with unknown or untrusted counterparties.[80] And its radical decentralization is what potentially makes smart contracts into substitutes for the state-based legal system, rather than merely screens in front of it. For example, a financial trading program that automatically buys certain stocks when their prices match a pre-defined algorithm could be described as a smart contract in some sense. 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 situation is novel because parties do not have that option. The transaction is irreversibly encoded on a distributed blockchain.

Smart contracts are possible with Bitcoin because its protocols include a scripting language that allows limited programmable logic to be incorporated into transactions. The vast majority of transactions on the Bitcoin blockchain are simple transfers of Bitcoins between accounts. However, when computers on the Bitcoin network process those transfers, they can be tasked with other function such requiring confirmation from multiple accounts. This allows for more complicated arrangements such as delaying payment until confirmation is received from a specified number of parties.

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.[81] The promise of Ethereum is almost comically broad: one article suggested it might "transform law, finance, and civil society."[82] 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 300 distributed apps built on the platform.[83] In one of the largest

[80] *See* Werbach, *supra* note 12 (describing the blockchain's "trustless trust" architecture).

[81] *See* Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper; D.J. Pangburn, *The Humans Who Dream of Companies That Won't Need Us*, FAST COMPANY, June 19, 2015, at http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them; 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, *at* http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn; Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That could Power the Internet of Things*, FAST COMPANY, May 21, 2015, at http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could-power-the-internet-of-things.

[82] Epstein, *supra* note 81

[83] *See* State of the Dapps, http://dapps.ethercasts.com (last visited Jan. 31, 2017).

crowdfunding campaigns ever, Ethereum raised over $18 million worth of Bitcoin in a sale of Ether, its internal cryptocurrency.[84]

The scripting language on a blockchain platform such as 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. 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. The Bitcoins may 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. The cost savings occur at every stage, from negotiation to enforcement, especially in the replacement of judicial enforcement with automated mechanisms.[85] If contracts are substantially cheaper and more efficient, more kinds of activities are opened up to contractual agreement. The second broad attraction of smart contracts is their fundamentally distributed nature. Those who wish to avoid trust in centralized private or governmental actors, whether for political reasons or otherwise, can now do so and still benefit from the advantages of contract.

Blockchain transactions are irrevocable. There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer. It is, however, possible to incorporate logic into a smart contract that allows for various forms of exceptions or conditions. Or enforcement could, in theory, be structured to allow for arbitration.[86] Such flexibility, however, has to be coded into the smart contract out the outset, and it takes away from the decentralization and efficiency that are the attractions of smart contracts to begin with.

Sometimes a smart contract may need to refer to facts in the world, such as when a contract pays out if a stock exceeds a certain price on a certain date. The Bitcoin blockchain knows nothing about stock prices; that information must be provided through an external data feed. In the language of smart contracts, systems that interpret such

---

[84] Nathan Schneider, *After the Bitcoin Gold Rush*, THE NEW REPUBLIC, 2015, http://www.newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle (last visited Jul 8, 2015).

[85] Of course, there is a tradeoff for the certainty of algorithmic enforcement, as will be discussed in Part IV, *infra*.

[86] 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/.

external feeds and verify contractual performance are referred to as oracles.[87] Unlike the blockchain, oracles are not fully decentralized. The contractual parties must, to some degree, trust the operator of the oracle and the authenticity of the data feed.

Using these capabilities, smart contracts can be employed for a wide variety of purposes. These could include not just simple financial arrangements but more complex vehicles such as wills[88] and crowdfunding systems (in which funds are only disbursed if projects hit a target threshold, and otherwise returned.)[89] Another category is so-called smart property, in which the rights associated with objects attach to the objects themselves. Networked door locks on shared cars (through a system such as Zipcar) could automatically open (only for that individual) when someone paid the access fee. Or, access to a leased car could be shut off from a delinquent lessee and given to the bank, but only until full payment of the principal. More broadly, with over 25 billion devices, from light switches to crop moisture monitors, expected to have internet connectivity in 2020, smart contracts would allow devices to operate autonomously, share resources, and exchange data without central management.[90]

Some blockchain advocates go farther. They envision smart contracts as the foundation of a new kind of economic entity, the distributed autonomous organization (DAO).[91] If a corporation is simply a nexus of contracts,[92] 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

---

[87] *See* Smart Oracles: A Simple, Powerful Approach to Smart Contracts, July 17, 2014, https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts

[88] *See* Morris, *supra* note 76.

[89] *See* Vigna and Casey, *supra* note 75. *See* Stan Higgins, *Bitcoin-Powered Crowdfunding App Lighthouse Has Launched*, COINDESK, January 20, 2015, *at* http://www.coindesk.com/bitcoin-powered-crowdfunding-app-lighthouse-launches-open-beta/

[90] *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/#!.

[91] David Johnston, et al, The General Theory of Decentralized Applications, DApps, https://github.com/DavidJohnstonCEO/DecentralizedApplications - the-emerging-wave-of-decentralized-applications; Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAGAZINE, Sept. 19, 2013, https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/.

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

trapping of a modern corporation, all running automatically in a completely distributed manner.

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 slightly more complicated—or at least ambiguous—than one might initially imagine. The first question we must necessarily answer is then: What do we mean by a "contract"?

According the standard legal definition, a contract is a promise or an agreement that is legally enforceable.[93] This definition, though widespread, has the unfortunate linguistic consequence of implying that agreements that turn out to be unenforceable weren't contracts to begin with. "Unconscionable contract," "fraudulent contract," "illegal contract" all become something like oxymorons.[94] And even commonplace judicial statements like, "To be legally enforceable, a contract must be supported by consideration,"[95] become essentially redundant.

What we care about, however, is whether smart contracts are contracts in the ordinary, folk meaning—whether enforceable or not.[96] At a general conceptual level, are smart contracts actually contracts?

---

[93] *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 1 (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.")

[94] *But c.f., e.g.*, United States v. Nunez, 673 F.3d 661, 664 (7th Cir. Ill. 2012) (" '[C]onspiracy' . . . is simply a pejorative term for a contract, both 'conspiracy' and 'contract' signifying an agreement, a meeting of minds. That is equally true when one person agrees to sell illegal drugs to another. Of course to be legally enforceable a contract requires certain formalities, which will not be found in a conspiracy. But their absence is of no moment; a criminal contract is unenforceable whatever form it takes.").

[95] *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.").

[96] 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?

One way to understand this question would be: Do smart contracts constitute promises or agreements that are *intended to be legally enforceable*? Contracts, on this understanding, are agreements that are intended to be legally enforceable, whether they turn out to be or not.[97] This definition has the advantage of avoiding the issues raised above: 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. What matters is what 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."[98] 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, however, the 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, however, to suggest that they are intended to be legally invalid. Rather, the question of legal enforcement should never come up. And, in this sense, smart contracts are not intended to be enforced in a legal proceeding. This lack of intent may lead one 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 courtroom.

This appearance, however, would be misleading. It is quite different to intend that a solution will not be needed than to intend that it will be unavailable. My car is not intended as a vehicle for escaping the zombie apocalypse, but, if the zombie apocalypse

---

[97] *See, e.g.*, EARL OF HALSBURY, 7 LAWS OF ENGLAND § 683 (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. By so intending, he has agreed to depart from the baseline rules (usually derived from tort or statute) that govern the mine-run of relationships between strangers.").

[98] 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 (1981) ("[I]t is clear that a mental reservation of a party to a bargain does not impair the obligation he imports to undertake.").

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. Intending that an agreement won't need to be enforced is not the same as intending that it not be enforceable.

A better way to think of a contract is as any agreement that is meant to have practical consequences on the rights and duties of the parties—i.e., is not merely aspirational.[99] This understanding makes irrelevant the fact that legal enforcement is not anticipated.[100] So the above difficulty is avoided. 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 a further difficulty. Even on this understanding, a contract requires—conceptually speaking—an exchange of promises or obligations. Do smart contracts involve promises or obligations? In a significant sense, the answer is "no." The smart contract sets in motion machinery that the parties cannot subsequently prevent. The fulfillment of the smart contract is not accomplished by some further action by a contracting party, but rather by the completion of this mechanical process. If someone 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 happen. In a similar way, a smart contract to transfer one bitcoin upon such-and-such event occurring is similarly not really a promise at all. It does 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."

Some of the computer scientists working on smart contracts appear 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…."[101] As

---

[99] *See, e.g.,* W. David Rankin, *Concerning an Expectancy Based Remedial Theory of Promissory Estoppel*, 69 U.T. 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.").

[100] *See* Gregory Klass, *Intent to Contract*, 95 VA. L. REV. 1437, 1460 (2009) (arguing that departure from any intention to create legally 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.");

[101] Buterin, *supra* note 81. *See also* Explainer: Smart Contracts, *at* https://docs.erisindustries.com/explainers/smart_contracts/ ("[S]mart contracts are neither particularly smart nor are they, strictly speaking, contracts."); Valerik Buterin, *Isn't Ethereum Just a*

this suggests, the language of "contracts" may appear misleading. The so-called 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. There's nothing being prospectively promised.

Nevertheless, we believe that smart contracts are, at the conceptual level, still contracts.[102] Though they might not constitute promises per se—depending on how we understand that idea—smart contracts are agreements that purport to alter the rights and duties of the parties. Not all contracts are executory. An agreement 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.

The smart contract, however, 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's no action left to be performed) nor executed (insofar as the result is yet to be accomplished). And this is what causes the conceptual difficulty. Smart contracts are both committing to something in the future, and yet not exactly making a promise either. As we discuss in below,[103] this hybrid between *ex ante* commitment and *ex post* enforcement is novel.

In the end, though, this complication raises more questions about our conceptual categories 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.

DSL for the Blockchain?, REDDIT.COM, https://www.reddit.com/r/ethereum/comments/31rnmh/isnt_ethereum_just_a_dsl_for_the_blockchain/ ("I now regret calling the objects in Ethereum 'contracts,' as you're meant to think of them as arbitrary programs and not smart contracts specifically".)

[102] For a more doctrinal analysis by an international law firm that reaches a similar conclusion, see Norton Rose Fulbright, *supra* note 9.

[103] *See infra* Part II.B.3.

There is one final difficulty to be 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 of the form "Party X agrees to do such-and-such." In general, a legal contract requires mutual assent, a so-called "meeting of the minds."[104] What this metaphor actually means is that both parties must have expressed assent to the contract.[105] That is, what is required are overt acts of assent.[106] Parties must engage in some expression that displays a shared understanding of the agreement and a shared intent to be bound by its terms. Can smart contracts—simply a chunk of code in a blockchain—constitute such shared expression?

There is nothing, so far as we can tell, that prevents an expression of mutual assent from being formulated in code. In general, mutual assent can take many forms, including a wide range of conduct so long as it clearly implies agreement.[107] There is no reason that this couldn't include expressions made in a code. As Harry Surden puts it, "At a minimum, contract laws do not explicitly prohibit expressing contractual obligations in terms of data. More affirmatively, basic contracting principles actively accommodate data-oriented representation." [108] 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 easily to satisfy the requirement of an expression of assent.

But 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: only one party places them on the blockchain.[109] That is, the default involves one party specifying a transfer to another if certain conditions are met. Out of

---

[104] *See, e.g.*, Krasley v. Superior Court, 101 Cal. App. 3d 425, 431 (1980) ("The essence of a contract is the meeting of minds on the essential features of the agreement.").

[105] *See* 1-4 CORBIN ON CONTRACTS § 4.13 ("The great majority of contracts are bargaining contracts, the purpose of which is to effect an exchange of promises or of performances. To attain this purpose, there must be mutual expressions of assent to the exchange. These expressions must be in agreement, but it is not necessary that they shall consist of identical words or identical acts. Their words and acts are called "expressions" because they 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.").

[106] *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.").

[107] *See* RESTATEMENT (SECOND) OF CONTRACTS § 4 & ill. 1& 2 (1981).

[108] Surden, *supra* note 20, at 656.

[109] http://coda.caseykuhlman.com/entries/2014/notes-from-my-ethereum-talk.html

this default, one could, of course, approximate a bilateral or multilateral contract through the creation of two or more interrelated unilateral contracts.[110] But two unilateral contracts are not precisely the same as a bilateral contract.[111] Fashioning the interdependence conditions in a way that would truly emulate a bilateral contract might be a challenge—even if a surmountable one—for smart contracts. For the purposes of this paper, we will leave this issue aside and generally focus on unilateral contracts. The same basic analysis would, we think, apply to bilateral contracts insofar as they might be formulated as smart contracts.

B. What's New Here?

Is a smart contract really any different than an ordinary one? The fact that the agreements are manifested in machine-readable code is not novel; nor is the possibility of automated performance based on rules-based judgments by computers. Both are features of data-oriented and computable contracts, which have been around for some time.[112] And just because smart contracts are being implemented today on the exotic technology of the blockchain doesn't necessarily mean they raise novel or interesting legal issues. As Frank Easterbrook has argued, new technologies don't necessarily call for new legal doctrines, when fact patterns are fundamentally unchanged.[113]

We consider two perspectives suggesting that smart contracts are just technological manifestations of familiar contractual processes: escrow and self-help. One focuses on the mechanism smart contracts use to ensure the execution of agreements; the other on the way they employ technology to impose a remedy outside of the court system. Each sheds light on the nature of smart contracts. However, neither fully captures the way they operate. What distinguishes smart contracts from pre-existing forms is that 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 just escrow arrangements with a digital veneer. In a typical escrow agreement, such as a house purchase, the buyer places funds in a special

---

[110] *Id.*

[111] *See* Francesco Parisi, Barbara Luppi & Vincy Fon, *Optimal Remedies for Bilateral Contracts*, 40 J. LEGAL STUD. 245 (2011).

[112] *See* Part I.A., *supra*.

[113] *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996). 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* (forthcoming 2016).

account. They can only be withdrawn and disbursed to the seller by the escrow agent after a successful inspection and resolution of any other pre-purchase issues. More generally, escrow suspends execution of a valid contract, and empowers a trusted third party to complete the process. Among other things, this approach overcomes the prisoners' dilemma when parties do not fully trust one another. Whichever one acts first is 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 places Bitcoins or other cryptocurrency tokens in a suspended state on the blockchain, where they cannot be spent until performance of the contract. The execution step may be fully automated, or implemented through multiple-signature verification, known as multisig.[114] In order for a multisig smart contract to execute, more than one party (typically two out of a possible three) must provide their private encryption keys.[115] Say that A wishes to purchase digital goods from B using a smart contract. The parties can use a multisig smart contract, requiring the digital signatures of two out of three parties: the buyer, the seller, and a trusted third party, such as an arbitrator. If the contract is performed in a satisfactory way, the buyer and seller sign, executing 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 pre-clearance 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.[116] BitHalo has implemented an escrow system for e-commerce transactions that avoids the participation of third parties entirely through the introduction of collateral.[117]

The fact that smart contracts can implement escrow agreements does not, however, make them identical to escrow. Conventional escrow depends upon a trusted third party. The parties themselves cannot serve as the escrow agents; they must turn to someone else,

---

[114] *See* Ben Davenport, *What is Multi-Sig, and What Can It Do?*, COIN CENTER, 2015, https://coincenter.org/2015/01/multi-sig/.

[115] *See* Narayanan, et al, *supra* note 60.

[116] *See* John Villasenor, *Could "Multisig" Help Bring Consumer Protection To Bitcoin Transactions?*, FORBES, March 28, 2014, http://www.forbes.com/sites/johnvillasenor/2014/03/28/could-multisig-help-bring-consumer-protection-to-bitcoin-transactions/ (last visited Jul 8, 2015).

[117] *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 (last visited Jul 11, 2015).

or a trusted firm. A smart contract reliant on an arbitrator gives up the decentralized trust that the blockchain makes possible. It is therefore more of a standard data-oriented contract. 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. There is no escrow agent.

2. Smart Contracts as Self Help

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.[118] 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."[119] He draws an analogy to starter interrupters, which are remote-controlled devices that can be installed in cars to prevent them from operating.[120] A creditor can invoke the starter interrupter when the lessee of an automobile 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 of Section 9-609 of the UCC.[121] A smart contract could serve the same function, by refusing to authorize operation of the car unless payment had been received.

Viewing smart contracts as self-help mechanisms accurately places the emphasis on the *ex post* enforcement function.[122] The blockchain can be used to record contractual provisions, execute contractual obligations, and perform intermediary functions such as escrow, but so can garden-variety digital contracts. It is when disputes arise or 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, take the place of judicial enforcement.[123]

Self-help, however, is a judicially supervised process.[124] Creditors who "disturb the peace" may be restrained from enforcing their self-help rights, or, as Raskin points out,

---

[118] *See* Raskin, *supra* note 16.

[119] *Id*. at 32.

[120] *See id*. at 28.

[121] *See id*. at 30.

[122] *See* Zoe 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).

[123] *See supra* Part I.C.

[124] *See* Sinel, *supra* note 122, at 66-67 ("[S]elf-help is a privilege of a limited sort…. The effects of these actions…are not ultimate determinations of the rights and obligations of the parties. Only

other legal obligations such as those of bankruptcy may trump them.[125] With a smart contract, there is no one to stop. The smart contract code is immutable once it is embedded in the blockchain. A smart contract could even include terms that are illegal, unconscionable, or otherwise legally unenforceable.[126]

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 a kind of appendage bolted onto the end of the contractual process to mitigate the risk of breach.

The analogy to starter interrupters breaks down on closer examination. The starter interrupter has nothing to do with the substance of the contract; it is a mechanism introduced after the agreement has been reached. This understanding, however, ignores the other aspects of smart contracts. Unlike a starter interrupter, a smart contract actually contains the terms of the agreement, transformed into machine-readable scripting code. The very fact that the agreement is enforceable algorithmically, without the participation of legal institutions, is a commitment represented in the smart contract. The self-help model paints too limited a picture of smart contracts.

At the same time, the self-help model is, in a way, too expansive: It attributes to smart contracts something they don't actually do. What performs the breach-limiting action is not the smart contract itself, but the distributed apparatus of the blockchain and its computing nodes. The smart contract is a component of a larger smart contract system. It is that system which ensures that, for example, the cryptocurrency tokens are transferred according to the contractual terms. Just as what distinguishes a legal contract from an

---

the state's legal institutions (which include legally recognized agreements between two parties – that is, contracts) can effect such a change… As such, self-help is not an alternative to the civil justice system but rather one small part of it.").

[125] *See* Raskin, *supra* note 16, at 31.

[126] 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 16, at 23. 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 isn't 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.

informal exchange of promises is introduction of the state to remediate *ex post*,[127] what makes a smart contract smart is the integration of the specific contractual terms with a general enforcement infrastructure. The distributed ledger software both instantiates the contractual terms and enforces the contractual obligations. These functions are distinguishable, but necessarily connected. In the self-help model, by contrast, one party enforces the agreement consistent with, but *outside* the legal machinery of contract law.

3. Smart Contracts as Entire Agreements

Both the escrow model and the self-help model view smart contracts as technical mechanisms overlaid on the basic contractual process. Escrow does so to facilitate performance, while self-help provides a remedy for non-performance. 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, however, 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.[128] There is, however, another element at work. 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. With other payment mechanisms such as checks or credit cards, an intermediary such as a bank must validate the transaction. This step introduces transaction costs and delay. It means the contracting process is no longer contained within the hardware and software of the vending machine. And it potentially changes the performance equation. The consumer can breach the agreement by instructing her credit card company to reverse the charge, even after receiving the product. The smart contract no longer governs the relationship between the parties.

Cash works for a vending machine, but not for a complex financial derivatives transaction, an international supply chain, or a major crowdfunding initiative. Only a limited subset of transactions in the world today are sufficiently localized, low-value, and low-velocity for cash to be a viable option.[129] This is another reason why Bitcoin and

---

[127] *See infra.*

[128] *See supra* note 37.

[129] Or, they are transactions the parties don't 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 I*, WIRED (Apr. 2015),

other cryptocurrencies are so 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, involves the complete exchange of value.

If I buy an ebook for my Kindle on Amazon.com, the company's computers transfer the book to my device, with associated digital rights to prevent additional copying. They also process my credit card and debit my account. Yet I can still ask Amazon for a refund, or dispute the charge with the credit card company. The contract with Amazon is executory — I'm trading the ebook for the promise to pay my credit card issuer. With a smart contract, by contrast, it's 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'm now asking them to return the money rather than preventing them from receiving it.

Because the exchange of value is entirely accomplished within the smart contract environment, there is no need to look anywhere else. In other words, the contract *is* the scripting code instructing the network on what to transfer and when. In the Amazon example, the site's computer system transfers the ebook and processes my credit card. Those machine instructions, however, are separate from the contract. If Amazon's programmers make an error, and I'm sent an entirely different ebook, there's no question the "real" contract controls. There may be questions about what constitutes that contract. Perhaps it's 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.

For the smart contract, in contrast, everything beyond the code is just an explanation. The blockchain is the distributed "computer" running that smart contract code. It's a necessary part of the agreement itself, whereas Amazon's servers are just tools to execute the human-made contract. Imagine that at the same time I place my order for the ebook 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. There would be an evidentiary question which version of the agreement controlled. In the smart contract context, such an inquiry would be meaningless. The written agreement cannot be part of the smart contract. If a court concludes it better reflects the parties' meeting of the minds, it would

---

http://www.wired.com/2015/04/silk-road-1 (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 II*, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2 (same).

be trying to supersede the smart contract, not interpret it. And then it would have to reverse the transfer of value *ex post*.

The notion that smart contracts can supersede legal enforcement has actually been tested in the real world.[130] A group of developers associated with Ethereum created a distributed crowdfunding system in mid-2016 called The DAO.[131] It was designed to implement the concept of a distributed autonomous organization, in which corporate governance and operations were conducted automatically through smart contracts.[132] Users pledged Ether (the Ethereum cryptocurrency) in return for tokens that gave them authority to vote on projects to be funded. Organizations seeking funding would sign up through another interface, and receive Ether if they received sufficient votes. Despite the novelty of the arrangement, Ethereum users pledged over $150 million of Ether in a matter of weeks after The DAO launched.[133]

The website where users signed up to participate in The DAO stated explicitly in its terms of service that the smart contract on the Ethereum blockchain was the controlling legal authority.[134] 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…."[135]

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.[136] Although clearly an attempt at theft, the hack was executed through a series of smart contracts that were

---

[130] 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.

[131] Christoph Jentzsch, DECENTRALIZED AUTONOMOUS ORGANIZATION TO AUTOMATE GOVERNANCE, https://download.slock.it/public/DAO/WhitePaper.pdf (last visited July 5, 2016).

[132] *See supra* note 91.

[133] Nathaniel Popper, *A Venture Fund with Plenty of 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.

[134] https://daohub.org/explainer.html.

[135] *Id.*

[136] Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES DEALBOOK (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; Michael del Castillo, *The DAO Attacked: Code Issue Leads to $60 Million Ether Theft*, COINDESK (June 17, 2016, 14:00 BST), http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/. The varying valuations of the hack are due to the floating exchange rate between Ether and dollars.

formally valid within the rules of The DAO. From the perspective of the smart contracting system, the transactions were perfectly legitimate. Thus, even though the stolen funds were temporarily quarantined in an account, not immediately disbursed, there was no legal or technical way to recover them without undermining the entire system. Even if a court ordered the funds returned, there was no one to carry out that order. Ultimately, the leaders of Ethereum project had to convince a majority of mining nodes to implement a "hard fork," which split the entire blockchain into two incompatible paths.[137] Only through this dramatic step, which effectively killed off The DAO and undermined confidence in the Ethereum platform, could the stolen funds be returned.

The DAO example shows the power of smart contracts, and also their limitations. Smart contracts could seemingly replace the legal system as enforcement mechanism for the 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

Ostensibly, smart contracts remove the role of courts as enforcement agents. One might say that the contract enforces itself, or that it is enforced by the code itself. What this means is that parties no longer have the escape hatch of litigation. Once the smart contract is made, machinery for its execution is unavoidably set in motion. The parties' opportunity to affect the transaction *ex post* will be cut off.[138] This may be a bit of an overstatement. Multisig, for example, may be used to give parties some persisting control over the execution of the contract.[139] Still, if smart contracts are to be a disruptive force in contracting, it turns on their ability to close off the possibility of breach of contract and the resultant litigation to enforce.

---

[137] 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, *in* Proceedings of the 36th IEEE Symposium on Security and Privacy, http://www.jbonneau.com/doc/BMCNKF15-IEEESP-bitcoin.pdf,, at 10.

[138] Note that this is consistent with the regular aim of business agreements to try to dictate remedies ex ante (e.g. mandatory arbitration, choice of law/forum, disclaimer of incidental/consequential damages, etc.).

[139] Narayanan, et al, *supra* note 60, at chapter 3, p. 12.

Does this mean that smart contracts can take the place of courts adjudicating contract cases? One can see how the argument would go.[140] 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 essentially obsolete—surpassed by mechanisms that can enforce obligations and thus serve the same function with greater efficiency and customization.

As we have discussed, we think there are reasons to be skeptical about whether the technology 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, one might still wonder whether its implementation would actually be an advance over courts or simply orthogonal. That is, one might wonder whether smart contracts are even theoretically equipped to replace the role of courts in contract law. Put simply, could smart contracts do what courts do only better? While it is easy to see why people have thought that they might, we disagree. That is, we think that contract litigation plays a role in our social system that smart contracts do not even purport to replicate.

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 smart contracts—Would smart contracts do what courts do only better?—introduces the reciprocal question about contract law—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. Which view one holds will inform how one thinks that smart contracts might interact with contract law. Ultimately, we mean to argue that the correct understanding of contract law makes clear that smart contracts cannot supplant the role that courts play. Smart contracts are not, even conceptually, a replacement for judicial contract adjudication.

But our argument in this section is also meant to be bidirectional. Insofar as many readers may already intuitively grasp that smart contracts can, at best, avoid courts but

[140] *See supra* notes 6-8 and accompanying text.

cannot substitute for them, this section is an argument that contract law should be understood in a particular way to accommodate that understanding.

A. Contract Law as Enforcing Promises

According to one natural view, contract law provides legal enforcement for promises.[141] When a promisor makes a commitment to a promisee, this commitment—the promise—generates an obligation to do the thing promised.[142] 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.[143] Contract law, the argument goes, serves to strengthen and support these moral obligations by creating corresponding legal obligations. At its core, what contract law does is make it the case that promisors are bound 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*.[144] For Fried, the capacity to make promises is a form of freedom, allowing parties to bind themselves and thus shape their obligations. By enforcing such voluntarily assumed obligations, the state supports the freedom of contracting parties. 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 promissory obligations in order to think that

---

[141] *See, e.g.*, CHARLES FRIED, CONTRACT AS PROMISE (1981).

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

[143] 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 524-525 (L.A. Selby-Bigge ed., 1967). Fried's account of contract law appeals to such a convention-based account of promises. FRIED, *supra* note 141, 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, ch. 7 (1998). For a picture of contract law built on such a reliance-based account of promissory obligation, see Joseph Raz, *Promises in Morality and Law*, 95 HARV. L. REV. 916 (1982). For further discussion of this philosophical debate, see WILLIAM VITEK, PROMISING (1993); Niko Kolodny & R.J. Wallace, *Promises and Practices Revisited*, 31 PHIL. & PUB. AFFAIRS 119 (2003).

[144] FRIED, *supra* note 141.

contract law's purpose is to provide legal obligations that correspond with the moral obligations of promises.[145]

The essential idea is simply that promises are an important part of human life and that contract law supports promising by offering legal recognition and enforcement. What contract law does is layer legal obligation on top of our moral obligations in order to bolster them. By making it the case that one must, legally, do what one has promised, we affirm that one ought to do what one promises 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 more successful the more that it truly affirms that promisors must do as they have promised. Elements of contract law that diverge from ensuring that parties keep their promises may, in this light, seem troubling.[146] In particular, the fact that contract law generally imposes only expectation damages rather than specific performance may appear problematic. [147] Specific performance would be better because it would more closely match our moral obligation, namely to do the thing promised.[148] 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 get us to do as we have promised.

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, the thought goes, aim to 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 do as they have promised, then a mechanism that automatically and completely

---

[145] *See, e.g.*, 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); 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).

[146] *See, e.g.*, Seana Valentine Shiffrin, *The Divergence of Contract and Promise*, 120 HARV. L. REV. 708, 749 (2007) ("advance[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").

[147] *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.")

[148] *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 this judgment.").

ensures performance may look like a triumph, at least insofar as it doesn't come at the expense of other freedoms.[149]

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

Of course, there's still room for concern, even within this picture of contract law as enforcing promises. First, one might suggest that smart contracts, by making performance inevitable, are essentially no longer promises at all. If so, then smart contracts wouldn't support our practice of promising. Whereas contract law supports promising by giving promisors a further set of reasons to perform, smart contracts do away with the need for reasons altogether and—the argument goes—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.[150] If we should, then smart contracts highlight the fact that contract law is about creating reasons and not 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 one lending the support. On this view, it is

---

[149] 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.*, CORBIN ON CONTRACTS § 1204, at 401 (2006) ("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 (2009).

[150] 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 it get myself to act, what I may seek is motivation rather than merely reasons.

essential that contract law strengthens promising through a political medium. In a contract case, the thought goes, we collectively express our affirmation of an obligation and lend our resources to enforcing that obligation.[151] 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.[152] 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 similar worries to those that have been expressed toward private arbitration or to penalty clauses.[153]

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

B. Contract Law as Voluntary Liability

A second view of contract law conceives it as designed to allow parties 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 with moral obligations.[154] Instead, contractual obligations can be fashioned where it is in the interest

---

[151] *See, e.g.*, Seana Valentine Shiffrin, *Paternalism, Unconscionability Doctrine, and Accommodation*, 29 PHIL. & PUB. AFFAIRS 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.").

[152] *See* Popper, *supra* note 40.

[153] *See, e.g.*, Owen M. Fiss, *Against Settlement*, 93 YALE L.J. 1073 (1983); Seana Valentine Shiffrin, *Remedial Clauses: The Overprivatization of Private Law*, 67 HASTINGS L.J. 407 (2016). 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.

[154] *See* Jody S. Kraus, *The Correspondence of Contract and Promise*, 109 COLUM. L. REV. 1603, 1617 (2009) ("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."); 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.").

of parties to create them. By creating legal liability, parties can create a distinctive kind of obligation that can serve any number of purposes, from enhancing agency[155] to facilitating efficient transactions.[156]

There are three key elements of this second view. First, contracts—as opposed to promises—essentially involve parties agreeing to legal liability if they fail to perform. The crucial element of contract law is that it allows certain agreements to be legally binding, where this means that they are subject to agreed-upon legal sanctions for breach. But whether or not any agreement is legally binding—and in what respect—is ultimately up to the parties.[157] Rather than seeing legal liability as parasitic on moral obligations, this view sees legal liability as the elective creation of the parties involved.

Second, the legal obligations of contract are a reflection of parties opting into liability. On this view, we can speak of legal obligations, as opposed to moral obligations. But, insofar as what parties opt into is a system of legal penalties, the legal obligations essentially describe those actions for which a legal sanction will attach.[158] Thus, by making it the case that one will face a sanction for failing to perform, one thereby generates an obligation to perform.

Third, because contracting is essentially about parties choosing to attach legal consequences to future actions, questions of contract law should be addressed to trying to determine what parties intended *ex ante* or would have chosen *ex ante*.[159] The basic question is what the parties would want, though perhaps subject to certain additional

---

[155] *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.")

[156] *See, e.g.*, Goetz & Scott, *Enforcing Promises: An Examination of the Basis of Contract*, 89 YALE L.J. 1261 (1980) (arguing that allowing people to bind themselves legally improves utility by allowing reliance among others).

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

[158] On this view, it would be incoherent to imagine parties agreeing to create a legal 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 obligations.

[159] *Cf.* Goetz & Scott, *Enforcing Promises*, *supra* note 156, 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.").

nuances.[160] 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.[161] The basic idea is that contract law is fundamentally about enabling transactional activity by creating a system of voluntarily binding oneself through opting into flexible and predictable consequences for breach.

If this is what contract law does, then smart contracting will again look like it could, in theory, supplant it. According to this second view, the fundamental purpose of contract law is to allow people to create reliable consequences enabling them to shape their behavior. The essential feature of contracts is that they must communicate information about what will be done in the future.[162] Efficient or agency-enhancing transactions can only take place if such communication is intelligible and trusted.

Smart contracts offer the possibility of highly reliable communication of future outcomes. This is true in two ways. First, because the agreed upon result occurs automatically, uncertainty both about performance and about judicial recognition are removed. 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, terms must be laid out in precise, operational terms.

In a well-functioning smart contract, interpretive questions are necessarily answered in determinative ways. In short, if you think that contract law exists to facilitate reliance through opting 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 may be a superior commitment mechanism.

---

[160] *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.").

[161] *See, e.g.*, Kraus, *supra* note 154, at 1648 ("Because they interpret promises according to the content most individuals do or would want, 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.* Goetz & Scott, *The Limits of Expanded Choice: An Analysis of the Interactions Between Express and Implied Contract Terms*, 73 CALIF. L. REV. 261 (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.").

[162] *See* Goetz & Scott, *Enforcing Promises*, *supra* note 156, 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.").

Of course, here again, there is room for certain concerns. In particular, one might worry that the *ex ante* information costs of determining what will happen in 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,[163] then the *ex ante* information costs might be mitigated and, to the extent that they persist, it would be a contingent matter in what situations they would 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, the two 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. Correspondingly, we believe that the above views about contract law's function are unsatisfactory. These two arguments are meant to be 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 possibly serve the same function as contract law.

Both the 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. Contract law aims to give 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 act. Contract law facilitates the creation of motivations, which need not correspond with our moral reasons, through the imposition of potential legal liability.

If one holds a motivation-creating view of contract law, then it will be natural to see smart contracts as supplanting contract law. After all, why create motives for action when one can ensure the action itself?[164] If contract law is about facilitating our actions going forward, then the smart contract seems like an appealing innovation.

---

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

[164] The same thing might be said about creating reasons for action, *see* note 150 *supra*, 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

But that's not what contract law is about. Contract law does not exist to alter our reasons going forward—though it surely does that—but rather it exists to adjudicate the justice of a situation *ex post*.[165] 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 but aimed at resolving disputes, taking the reasons as already given.

Here's a simple example to illustrate the difference among the three views. Suppose that 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. She has created reasons to perform by opening herself up to moral sanctions. Contract law would allow her, if she would like, to subject herself to even more accountability—legal accountability. Thus, she could create more—or different—motivation to perform by opening herself up to a new set of sanctions. The difference between these two answers 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.

But here is an altogether different answer about what contract law adds: Contract law creates a forum to determine what happens if Abby doesn't perform.[166] On this view, contract law doesn't 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

---

motivation. We leave that possibility very open. But, if so, then this again highlights the inability of smart contracts to supplant contract law.

[165] *Cf.* RESTATEMENT (SECOND) OF CONTRACTS ch. 16, introductory note (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.").

[166] This idea appears to be an element of recent civil recourse theory. *See* Nathan B. Oman, *Consent to Retaliation: A Civil Recourse Theory of Contractual Liability*, 96 IOWA L. REV. 529 (2011); Benjamin C. Zipursky, *Civil Recourse, Not Corrective Justice*, 91 GEO. L.J. 695 (2003). 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.

to pay the money back.[167] Contract law adds something *ex post* to deal with failure. It's not about seeing to it that she performs but about responding if she doesn't.

When one views contract law in this way, then it is apparent that smart contracting doesn't 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—take the place of contract law. At best, smart contracts might reduce the need for contract litigation. But that wouldn't mean that they are serving the same function in a superior fashion.[168] Rather, it would mean a shift to an altogether different mode of interaction, and one not clearly superior.

IV. SMART CONTRACTS IN PRACTICE

If smart contracts are doing 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 Nick Szabo's unfortunate choice of terminology two decades ago. If he had called his idea "intelligent agents" or "virtual vending machines," would there be any reason to examine the legal implications further? We believe there would. 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 still nominally subject to contract law. Problems are likely to arise. These in turn will produce responses which have 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.[169] This view is overly optimistic.[170] While the potential benefits of smart

---

[167] 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.").

[168] 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 ("Habitual texters . . . don't get to practice the art of interpreting nonverbal visual cues.").

[169] *See, e.g.*, Tapscott & Tapscott, *supra* note 6, 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 76 ("Someday, these programs may replace lawyers…."). Andrew Keys, Memo from Davos: We Have a Trust Problem. Personal

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.[171] 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 the 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 eliminating them. Smart contracts are likely to face two kinds of problems: practical and doctrinal. These difficulties will create pressure for responses. Some 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.

A. Imperfections of Algorithmic Enforcement

There are significant practical limitations in replacing human enforcement of agreements with software running on the blockchain. Things simply don't always go according to plan.[172] Anyone who has ever 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

---

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 ("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.").

[170] 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.

[171] *See* MARY WOLLSTONECRAFT SHELLEY, FRANKENSTEIN, OR, THE MODERN PROMETHEUS (1818). *Cf.* Andrea M. Matwyshyn, *Corporate Cyborgs and Technology Risks,* 11 MINN. J. L, SCIENCE & TECH. 573 (2010) (describing firms in the securities industry increasingly dependent on information technology as "corporate cyborgs.").

[172] *See* Lauren Henry Scholz, *Algorithmic Contracts* (forthcoming) (manuscript at 7) (online at https://ssrn.com/abstract=2747701) ("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").

on top of them may not be.[173] The failure of The DAO should be a cautionary note for smart contract developers.[174]

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 which can readily be specified precisely.[175] A contract that my connected car will be unlocked 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. On 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.[176]

Building a computerized system able to interpret smart contracts with similar levels of understanding to humans is effectively a challenge for artificial intelligence.[177] And it is one unlikely to be solved any time soon.[178] Despite great advances in machine learning,

---

[173] Peter Vessenes, co-founder 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 (May 18, 2016), http://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/. Even for commercial software, the industry average is 10-15 errors per 1000 lines of code. *See* STEVE MCCONNELL, CODE COMPLETE: A PRACTICAL HANDBOOK OF SOFTWARE CONSTRUCTION (2nd Ed., 2004).

[174] *See supra* note 136.

[175] *See* Surden, *supra* note 20, at 682-83.

[176] 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* text at note 116. At some point, however, doing so transforms the smart contract into a conventional contract with an arbitration clause, eliminating the alleged benefits of the approach.

[177] Steve Omohundro, *Cryptocurrencies, smart contracts, and artificial intelligence*, 1 AI MATTERS 19–21 (2014).

[178] "The conventional view has been that the automation of contract monitoring or compliance is beyond the capability of contemporary technology." Surden, *supra* note 20, at 632,

computers don't have the degree of contextual, domain-specific knowledge or subtle understanding required to resolve contractual ambiguity. And smart contract platforms such as Ethereum are vastly less sophisticated in this regard than state-of-the-art artificial intelligence systems such as IBM's Watson.

Even if the smart contract operates exactly as designed, it may produce sub-optimal results (either in the minds of one or both parties, or as a matter of economic efficiency) because it is fixed. Sometimes, for example, non-performance is the desirable outcome. Much has been made of the idea of efficient breach.[179] If a builder contracts with a carpenter to custom-make woodwork for a new home, but notifies the carpenter prior to initiation of the work that the home will not be built, nonperformance and compensation to the carpenter may be the best result. One interpretation is that contract law is designed to facilitate such nonperformance, at least insofar as the legal default rules of contractual remedies stood behind the parties' negotiation.[180] But, one need not accept the theory that the law sanctions efficient breach to appreciate that the law does not lock parties into performance.[181]

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 are the kinds of imprecise terms that are difficult to specify in computer code. In other cases, parties may wish to enter into a mutually advantageous alteration of a contract prior to performance. Under standard contract law, such modifications are unproblematic.[182] For smart contracts, they pose a difficulty. Upon agreement, contract is

---

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).

[179] *See, e.g.*, Robert 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."); RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 13-14 (1998).

[180] *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.").

[181] *See* Cornell, *supra* note 14, 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 judges breach of contract permissible when the costs are high enough. Contract law simply does not determine permissibility.").

[182] *See* RESTATEMENT (SECOND) OF CONTRACTS § 89.

locked into place and secured through 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 encode when and how parties might be permitted to modify set terms of a smart contract.

As the literature on relational contracts recognizes, contracts are often more than a one-shot interaction between parties, followed by performance or judicial resolution of a dispute.[183] Instead, they are elements of ongoing relationships. Both the parties and courts view the contract in light of social as well as 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.[184] Smart contracts attempt to atomize the contractual process. They formally strip away both the time dimension of interactions among the parties, and the uncertainties of future judicial resolution. Yet in the real world, they 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 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: meeting of the minds (defined as offer and acceptance), consideration, capacity, and legality.[185] But there are still a host of potential problems lurking. At virtually every turn, there is the possibility that 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

---

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

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

[185] *See, e.g.*, Cohn v. Fisher, 287 A.2d 222 (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 (1981).

smart contract ensures a true meeting of the minds; nothing ensures consideration; and so on. In what follows, we describe a number of ways that smart contracts might operate problematically contrary to the law of contracts.

1. Problems with Meeting of the Minds

A smart contract is computer code representing an agreement among two or more parties, so one question might be whether it truly represents a meeting of the minds. Computers, after all, don't have minds, at least not outside the realm of science fiction. This objection is quickly overcome. In modern contract law, offer and acceptance are evaluated objectively.[186] That is to say, what counts is evidence that both parties intend to be bound, not some indicia of internal mental states. The very fact that parties submit their cryptographic private keys to commit resources to a smart contract is proof of such a commitment.

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.[187] If the smart contract refers to cotton delivered by the ship *Peerless* but there are two—or seventeen—ships of that name, standard contract law can hold the agreement unenforceable.[188] The smart contract, however, would go ahead and execute.[189] In a unilateral contract like this, the mistake might not even need to be mutual for a court to rescind it.[190] In other words, it is possible that there might be an executable smart contract that did not satisfying 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*.

---

[186] *See supra* note 98 and accompanying text.

[187] *See* RESTATEMENT (SECOND) OF CONTRACTS §§ 20(1) & ill. 2, 152 (1981).

[188] *See* Raffles v. Wichelhaus, 159 Eng. Rep. 375 (Ex. 1864). For the fact that there were seventeen 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 (1989).

[189] 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 *status quo ante*.

[190] *See, e.g.*, Conduit & Foundation Corp. v. Atlantic City, 64 A.2d 382, 384 (N.J. Super. Ct. 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, S. P. M. & O. R. Co. v. Washburn Land Co., 165 Wis. 125 (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.")

The basic problem here is that smart contracts aren't really smart—at least not in the way that contract law is smart. They 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 don't specify an outcome for every possible state of the world.[191] 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 is when the contract itself is clear, yet doesn't represent the intent of the parties. A party may enter into an agreement due to fraud or duress. In such a situation, performance may be excused.[192] 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. The only recourse for someone fraudulently induced to enter in a smart contract would be to sue for restitution of the ill-gotten gains. Fraud, however, is significantly different as a cause of action than as an affirmative defense.[193] And duress is not a cause of action at all.

2. Problems with Consideration

Similar problems arise with respect to consideration, the second basic requirement for an enforceable contract. The primary practical effect of consideration is to distinguish contracts from unenforceable gifts.[194] All promises may create moral duties, but not all create legal obligations. With smart contracts, however, there is no test for consideration. A typical smart contract will involve some consideration that induces the reciprocal promise. However, there is nothing stopping someone from committing a gift promise to the blockchain. Such a promise will be executed irrevocably in the same manner as any other smart contract. The rest of consideration doctrine, such as the distinction between

---

[191] *See* Sanford J. Grossman & Oliver D. Hart, *The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration*, 94 J. POLITICAL ECON. 691 (1986); Oliver D. Hart & John Moore, *Property Rights and the Nature of the Firm*, 98 J. POLITICAL ECON. 1119 (1990).

[192] *See* RESTATEMENT (SECOND) OF CONTRACTS § 162 (fraud); *id.* § 175 (duress).

[193] *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 […]").

[194] *See* Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 815 (1941); JOSEPH M. PERILLO & JOHN D. CALAMARI, CALAMARI AND PERILLO ON CONTRACTS 149-50 (6th ed. 2009)

adequacy and sufficiency, similarly goes by the wayside when there is no means to test enforceability prior to execution.[195]

The absence of consideration from smart contracts sheds further light on how they differ from legal contracts. Consideration doctrine is a data point that contract law exists to provide remedies for breach, not to generate *ex ante* obligations.[196] If the point of contract were to enforce promises or all parties to voluntarily advert to liability, why not allow them to make binding gift promises? From its *ex post* vantage point, contract law may distinguish unenforceable gifts from mutual legal obligations. Smart contracts, by contrast, 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.[197] 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 in the same way as they are restricted from having credit cards or accounts on payment services such as PayPal. And if someone digitally signs a smart contract while dead drunk, or another person exploits their circumstances to get them to do so, there is no opportunity for subjective evaluation by the other party.

The absence of a capacity test raises a somewhat 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 is assumed to represent 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.[198] Identity, however, is a rich concept, requiring layering

---

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

[196] *See supra* Part III.C.

[197] *See* RESTATEMENT (SECOND) OF CONTRACTS § 12. As with meeting of the minds, this is an objective test. *See* RESTATEMENT (SECOND) OF CONTRACTS § 12(1) (1981) ("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").

[198] *See* L. Jean Camp, *Digital Identity*, IEEE TECH. & SOC'Y (Fall 2004) at 34.

of various capabilities for authentication, access, and so forth.[199] Moreover, even if a key uniquely belongs to an individual, the two 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, it may designate a persistent digital identity hiding the associated real-world person (pseudonymity) or it may give no information at all about identity (anonymity).

Is it even 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.[200] There, however, it is generally not difficult to view the computers as agents for their human programmers, who specify the conditions under which they can contract. While there may be practical difficulties, they are not so different from those 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. Can they be said to have the capacity (in the legal sense) to perform it?

The analysis here connects with the conclusion above that smart contracts are not promises, even if they are contracts.[201] That may be fine conceptually, but as the foregoing discussion shows, things start to unravel when viewed doctrinally. Law bakes in assumptions about the human nature of contract. We may have no difficulty imagining a contract that isn't really a contract, but when subjected to the more rigorous analytical tests of contract law, the concept becomes more difficult to maintain.

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 example, a price fixing conspiracy implemented through a series of smart contracts that adjust prices in lockstep.[202] The participants could be prosecuted under antitrust law, but the smart contracts would continue to operate. There is also no mechanism to stop a smart contract from implementing a term that is unconscionable, or incorporates

---

[199] *See id.*

[200] *See supra.*

[201] *See supra* Part II(A).

[202] This scenario of an algorithmic conspiracy has in fact been suggested by competition law experts. *See* ARIEL EZRACHI & MAURICE STUCKE, VIRTUAL COMPETITION (2016).

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; they will be performed regardless.

The legality test and the various public policy rules hint that contract, generally considered a bastion of private law, contains a penumbra of public law. Again, this reinforces the view of contract as an adjudicative mechanism, rather than one concerned principally with reasons and obligations.[203] Legal adjudication is a public function, drawing on the coercive power of the state. Individuals acting together may have no problems with effectuating a scheme in derogation of public policy, but the state is something more than a collection of individuals. It is Hobbes' Leviathan, granted an extraordinary monopoly on violence for the very purpose of preventing the war of all against all.[204] Smart contracts detach the id of private ordering from the superego of public enforcement.

The hacking of The DAO illustrates the problem with contracts that have no check on illegality.[205] The hack was simultaneously valid as an enforceable smart contract within the bounds of the software system and 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 difficulty, legally or practically, 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, it was like using a bazooka to shoot a mouse; the collateral damage was significant.

And even if a hard fork is effective, it transfers final adjudication from the institution of the courts to the polity of validation nodes. A hard fork stands or falls on whether a majority of mining power in the blockchain network adopts it. This is not how contract works. 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 in some cases for legislative modification going forward. The limitations of direct democracy are familiar to anyone who has read the *Federalist Papers*.[206] And miners' interests may be even further removed from those of the community as a whole than factions in a democracy.

---

[203] *See supra* Part III.

[204] *See* Hobbes, *supra* note 3.

[205] *See* Popper, *supra* note 136.

[206] *See, e.g.*, THE FEDERALIST, No. 10, at 54-55 (James Madison) (Modern Library ed., 2000).

The point of this digression is not 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. And we have no way of knowing how popular smart contracts will become, let alone how frequently controversies such as 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 the previous Part, 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 must necessarily be 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 unproblematically.

1. Best Practices

The parties entering into smart contracts are not powerless to avoid their shortcomings. Knowing they cannot rely on the judicial decision-makers to fill gaps, one can expect them to put more effort into contract design and drafting.[207] And just as 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.[208] Technical mechanisms can also be employed to lessen the rigidity of smart contracts. Giving authority to human oracles who decide whether the factual basis for performance has been met,[209] or employing arbitrators who resolve disputes through a multisig arrangements,[210] are ways to avoid some of the draconian implications of fully self-enforcing agreements.

---

[207] *See* Robert E. Scott, *The Case for Formalism in Relational Contract*, 94 NW. U. L. REV. 847 (1999) (making a similar point about parties entering into open-ended relational contracts).

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

[209] *See supra* note 87.

[210] *See supra* note 114.

Already, organizations involved in the development of smart contract platforms are starting to create templates that embody best practices for smart contract drafting.[211] Using these templates, parties could avoid repeating mistakes of 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,[212] could be programmed to automatically offer templates based on the desired type of agreement. Some default terms, such as an opportunity for mutual modification prior to execution, could even be made mandatory to issue a smart contract on a particular platform. Even if the platforms are not subject to any legal duties with regard to 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 be realized. Surely the technical mechanisms for improving the quality of smart 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 truly eliminate litigation. Litigation—like nature—will find a way. Parties will inevitably still feel hard done at times, and they will inevitably still bring those complaints to court. The difference, however, will be the stance that the litigation will take. Rather than complaining parties seeking to have alleged promissory obligations fulfilled, complaining parties will now be seeking to undo or reverse completed transactions. Litigation will persist, but it will be shifted from claims of breach to claims of restitution.

One might think that this effectively shifts contracts from liability rules to property rules.[213] But that's not quite right—one could have a smart contract that awarded liability damages in a self-executing way. Rather the difference is between *ex ante* enforcement and

---

[211] *See* Christopher D. Clack et al, Smart Contract Templates: Foundations, Design Landscape and Research Directions (Aug. 4, 2016), https://arxiv.org/pdf/1608.00771v2.pdf; Ian Allison, *Barclays' Smart Contract Templates Stars in First Ever Public Demo of R3's Corda Platform*, INT'L. BUS. TIMES (Apr. 18, 2016 15:45 BST), http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329.

[212] *See* Raskin, *supra* note 16.

[213] *See* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

ex post adjudication. What we have tried to illustrate is that it is a mistake to conceive of these as simply two different forms of "enforcement."[214]

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 role of the parties is reversed. In an action for breach, it is the non-performing party seeking to enforce a transaction, whereas, in an action for restitution, it is the performing party who seeks to reverse the transaction. With the reversal in who stands as plaintiff comes a shift in 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 claims of fraud, repugnance to public policy, or a gift without consideration are the basis for the action, the balance of equities may shift in undesirable ways.

Those seeking redress for injuries suffered due to smart contracts may be forced in many cases to plead actions beyond even 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. One is a tort and the other is an affirmative defense in contract, and the legal requirements are different. Moreover, in practice, such litigation may unfold quite differently as the focus may shift from the contract to the technical structures associated with it.[215] 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 her key, or perhaps computer passwords protecting it. Law enforcement agencies have done just that, when pursuing proprietors of Bitcoin exchanges promoting illegal activity such as drug trafficking.[216] If that's the model, however, we've strayed quite far from the private law domain of contract.

---

[214] *See supra* Part III.

[215] 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 (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/. 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, *Uber 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. Whether this waiver is enforceable is another question.

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

3. Regulation

Indeed, the paradoxical result of smart contracts may be to expand the scope of government intervention into what has traditionally been the 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 it to the front end of the process. The only way to ensure smart contracts do not go down problematic paths is to regulate them.

It is a myth that the blockchain is inherently unregulable.[217] Any particular distributed ledger system may be more or less decentralized, and more or less anonymous, based on technical design decisions. Bitcoin and Ethereum are permissionless systems, meaning there is no super-entity authorized to accept or reject participation in the mining network.[218] Other smart contract platforms, such as the Corda system for inter-bank transactions, only recognize trusted nodes, such as member banks.[219] This makes them less resistant to government intervention or private domination, but those are lesser concerns of bank than libertarian-leaning engineers. A Corda smart contract could easily be subject to regulatory oversight, such as the Anti-Money Laundering and Know Your Customer regulations that mandate identification of bank customers.[220] Even for a permissionless system, centralized intervention is not

---

[217] *See* JERRY BRITO, *Forward*, *in* THE LAW OF BITCOIN (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 (May 19, 2014), http://reason.com/archives/2014/05/19/bitcoin-remains-a-tool-for-freedom-even ("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 17, at 4 ("there 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, 9:00 AM), http://www.coindesk.com/why-regulating-bitcoin-will-not-work ("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]").

[218] *See* Tim Swanson, Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems (Apr. 6, 2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf (explaining the distinction between permissioned and permissionless blockchains).

[219] *See id.;* Michael del Castillo, *R3 Announces New Distribution Ledger Technology Corda*, COINDESK (Apr. 5, 2016, 22:45 GMT), http://www.coindesk.com/r3cev-blockchain-regulated-businesses/.

[220] *See* Ian Allison, *R3 Develops Proof-of-Concept for Shared KYC Service with 10 Global Banks*, INT'L. BUS. TIMES (Nov. 10, 2016, 15:15 GMT), http://www.ibtimes.co.uk/r3-develops-proof-concept-shared-kyc-service-10-global-banks-1590908; Aleya Begum, *R3's Corda uncovered: It's not blockchain*, GTR (Oct. 1, 2017), http://www.gtreview.com/magazine/volume-15issue-3/r3s-corda-

impossible, only difficult, as shown by the Ethereum hard fork to resolve The DAO hack.[221]

A perhaps more apt parallel is 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.[222] A digital signature, however, is not really a signature at all. It's a private key, generating an associated public key. It took legislation, the E-SIGN Act, to preempt contrary state law and ensure that rules requiring signatures could be satisfied with their digital analogues.[223] The legal effects and limitations of digital signatures are therefore defined not by handwriting specialists, but by government.

There are many scenarios under which 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 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.[224] The kinds of smart contracts parties can form will depend on the functionality and interfaces of the available tools. The situation recalls the fate of peer-to-peer (P2P) file-sharing systems such as 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, they were still liable if set up to induce them.[225]

Regulation will not be limited to illicit activity. Various agencies, including the Federal Trade Commission (FTC), Securities and Exchange Commission, and Consumer Financial Protection Board have authority to prevent unfair or deceptive practices, for example. This extends to situations where companies do not intend consumer harms, but

---

uncovered-not-blockchain ("Corda takes a different approach. By default, information about transactions is only shared with those parties to a transaction").

[221] *See supra* TAN 136.

[222] *See* John Schwartz, *E-Signatures Become Valid for Business*, N.Y. TIMES, Oct. 2, 2000, at 1; Tim Squitieri and Paul Davidson, *E-Signatures Seen as Big Boon to Business: Companies Expect to See Huge Savings*, USA TODAY, June 15, 2000, at 7A.

[223] Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-229, 101.114 Stat. 464 (2000). *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).

[224] *See* Raskin, *supra* note 16 (suggesting that illegal smart contracts be subject to regulation).

[225] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

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 several losses of customer data.[226] 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.

To some degree, this is a familiar story. Where freedom of contract stands in the way of important public policy objectives, it may be forced to give ground. That occurred most famously when the New Deal eventually broke through the *Lochner* court's resistance to economic regulation.[227] 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.

D. Conclusion

Our goal has been to analyze smart contracts from the perspective of law—and vice versa. Though there is significant evidence they 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. Finally, the very act of unpacking smart contracts may help to anticipate—and thus mitigate—potential difficulties.

Smart contracts are just one example of a larger trend of computerized technologies purporting to displace or replace human decision-making.[228] In areas such as hiring, financial decisions, and copyright enforcement, algorithmic systems are touted for their speed, efficiency, and reliability, in contrast to mistake-prone and potentially biased humans. And indeed, the benefits are considerable. Yet it quickly becomes clear that the

---

[226] *See* F.T.C. v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 615 (D.N.J. 2014), motion to certify appeal granted (June 23, 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015) (upholding the FTC's action).

[227] *See, e.g,* Nebbia v. New York, 291 U.S. 502, 510 (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.").

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

machines are prone to their own errors and biases. [229] And the introduction of algorithmic systems creates challenges for legal and practical accountability.[230] As a result, both legal scholars and computer scientists are developing techniques to promote fairness and transparency in these decisions.[231] 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's happening. However, contract law may learn something about itself from its new challenger.

---

[229] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[230] Maayan Perel & Nica Elkin-Koren, *Accountability in Algorithmic Copyright Enforcement*, __ STANFORD TECH. L. REV. ___ (forthcoming); Pasquale, *supra* note 229.

[231] *See* Joshua A. Kroll et al, *Accounable Algorithms,* 165 U. PENN L. REV. ___ (forthcoming 2017); Barocas & Selbst, *supra* note **Error! Bookmark not defined.**; Michael Feldman, et al, *Certifying and Removing Disparate Impact*, Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (2015); Nicholas Diakopoulos, *Accountability in Algorithmic Decisionmaking*, COMMUNICATIONS OF THE ACM, February 2016, at 56.