September 2019

Smart Contracts and Consumers

Tatiana Cutts

London School of Economics and Political Science

Follow this and additional works at: <https://researchrepository.wvu.edu/wvlr>

Part of the [Commercial Law Commons](#), and the [Contracts Commons](#)

Recommended Citation

Tatiana Cutts, *Smart Contracts and Consumers*, 122 W. Va. L. Rev. (2019).

Available at: <https://researchrepository.wvu.edu/wvlr/vol122/iss2/4>

This Article is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact ian.harmon@mail.wvu.edu.

SMART CONTRACTS AND CONSUMERS

*Tatiana Cutts**

ABSTRACT

“Smart contracts” are a way of using computers to make contracts unbreakable. Contracting parties do not need to trust one another to perform or rely upon intermediaries to enforce performance. Performance is guaranteed. This is supposed to be a victory for the ordinary person—a clever socio-economic application of cryptography that strips power from companies and governments and gives it to consumers. But it turns out that less trust does not mean more freedom, or better bargains. The law of contract supports valuable relationships both by enforcing duties and by allowing parties to escape the consequences of ill-formed contracts and oppressive terms. Smart contracts remove these safeguards; consumers may be bound, inexorably and without recourse, to contracts that lack any virtue. The lesson of smart contracting is clear and urgent: when we design the future of commerce, we should direct our resources towards building, not emaciating, relationships of trust.

I.	INTRODUCTION.....	390
II.	EXPLAINING “SMART CONTRACTS”.....	395
	A. <i>Automating Asset-Sales: Creating Confidence in Counter Performance by Limiting the Power for Intervention.....</i>	399
	1. Buying and Selling Assets	399
	2. Automating Asset Sales	401
	3. Buying and Selling Digital Assets	402
	4. Automating Digital Asset Sales	403
	B. <i>Blind Consensus Protocols: Understanding the Political Model and Practical Ramifications of Blockchain Technology.....</i>	404
	1. Blind Consensus.....	405
	2. Crypto-Assets and Block-Chains	409
	C. <i>Smart Contracts: Negatively-Automated</i>	

* Assistant Professor, London School of Economics and Political Science (LSE). I am grateful for comments from Andrew Murray, and have also benefited from numerous invaluable conversations with (amongst others) Michèle Finck, Heikki Marjosola, Eva Micheler, Philipp Paech, Edmund Schuster, Andrew Summers, and Frederick Wilmot-Smith.

	<i>Asset Sales and the Digital Environment</i>	411
	1. Putting It All Together:	
	Negatively-Automated Asset Sales.....	411
	2. Digital Contracts for Public Networks.....	413
	3. Three Smart Contracts; One Core Case	414
III.	JUSTIFYING SMART CONTRACTS.....	418
	A. <i>Smart Contracts and Legal Contracts</i>	418
	1. What Is a Contract?.....	420
	2. Code and Contracts	422
	3. Code and Ownership.....	425
	4. Language Games.....	428
	B. <i>Smart Contracts and the Law of Contract</i>	429
	1. What Is Contract Law?	430
	2. Smart Contracting and Contract Law.....	432
	C. <i>Are Smart Contracts a Good Thing?</i>	436
	1. Positively-Automated Contracts	436
	2. Negatively-Automated Contracts.....	438
IV.	CONCLUSION	444

I. INTRODUCTION

What should the law do about autonomous machines?¹ Lawmakers have grappled with that question for thousands of years. Two millennia before Roman Law emerged in a systemic form,² Babylonian codes apportioned liability for various devices that were (in whole or part) self-operating.³ As technological practices have matured, attention has turned to the questions raised by *digital* automation.⁴ And as computers have become more closely integrated into

¹ “Automation” is “the fact of making something . . . automatic.” *Automation*, OXFORD ENG. DICTIONARY, <https://www.oed.com/view/Entry/13468?redirectedFrom=automation#eid> (last visited Sept. 25, 2019). “[A]utomatic” is either “self-generated, spontaneous,” “self-acting; having the power of motion within itself” or it is (more specifically) “having intrinsic activity that is not dependent upon external stimuli.” *Automatic*, OXFORD ENG. DICTIONARY, <http://www.oed.com/view/Entry/13464?redirectedFrom=automatic#eid> (last visited Sept. 25, 2019).

² Internal evidence suggests that the Institutes of Gaius were completed around A.D. 161. BARRY NICHOLAS, AN INTRODUCTION TO ROMAN LAW 36 (1976).

³ The Code of Hammurabi contains several rules that concern, inter alia, man-made dams that had not been maintained “in proper condition.” *The Code of Hammurabi*, LILLIAN GOLDMAN L. LIBR., <http://avalon.law.yale.edu/ancient/hamframe.asp> (last visited Sept. 25, 2019). Other rules concern partially self-operating devices, including boats and horse-drawn carts, and wholly autonomous “property,” such as slaves. *Id.*

⁴ For one of the best-known treatises concerning the regulation of “cyberspace,” see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

commercial practice and social habit, the more complex these questions have become: Can code embed moral values?⁵ To what extent should code writers be held accountable for their creations? How does online automation affect the way in which standards of behaviour are regulated?⁶

The novel and much-celebrated practice of “smart contracting”⁷ brings such questions into sharp focus. The promise is broad and optimistic—better facilities for expressing contractual rights and duties in computer code and more sophisticated methods for making sure that that code operates as intended.⁸ In this way, smart contracts oil the wheels of digital commerce.⁹ But a purely economic account of smart contracting would be incomplete. A core ideological commitment of this contractual renaissance is to empower individuals to bargain on a peer-to-peer basis, without so-called “trusted third parties”¹⁰—whether commercial intermediaries (such as banks and marketplace-hosts) or public authorities (such as courts).

⁵ One recent manifestation of that question arises in the context of self-driving cars. *See generally* LANCE ELIOT, *AI SELF-DRIVING CARS BREAKTHROUGHS: PRACTICAL ADVANCES IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING* (2018); Jessica S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit The Brakes on Self-Driving Cars*, 31 *BERKELEY TECH. L.J.* 851 (2016); Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 *CALIF. L. REV.* 1611 (2017).

⁶ And if so, which states, and when? The questions of jurisdiction, or “choice of law,” are particularly fraught. *See generally* Paul Schiff Berman, *Towards a Cosmopolitan Vision of Conflict of Laws: Redefining Governmental Interests in a Global Era*, 153 *U. PA. L. REV.* 1819 (2005) (discussing this question as it relates to the internet).

⁷ The term “smart contract” was coined by Nick Szabo in a blog post entitled “Smart Contracts.” Nick Szabo, *Smart Contracts*, PHONETIC SCI. AMSTERDAM (1994), <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> [hereinafter *Smart Contracts*] (describing a smart contract as “a computerized transaction protocol that executes the terms of a contract”); *see also* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, SATOSHI NAKAMOTO INST. (1997), <https://nakamotoinstitute.org/formalizing-securing-relationships/>.

⁸ PRIMAVERA DE FILIPPI & AARON WRIGHT, *BLOCKCHAIN AND THE LAW: THE RULE OF CODE* 78–80 (2018) [hereinafter *THE RULE OF CODE*]. Smart contracts are “more dynamic”; “what makes smart contracts unique is that they grant contracting parties new tools to reduce monitoring costs . . . any . . . performance obligations will only execute according to the terms and conditions expressly provided for in the underlying code.” *Id.* at 80.

⁹ Kevin Werbach & Nicholas Cornell, *Contracts Ex Machina*, 67 *DUKE L.J.* 313, 318 (2017). “Algorithmic enforcement allows contracts to be executed as quickly and cheaply as other computer code. Cost savings occur at every stage, from negotiation to enforcement, especially in replacing judicial enforcement with automated mechanisms.” *Id.* at 335.

¹⁰ This term was used by an author or group of authors writing under the pseudonym “Satoshi Nakamoto” in Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, at 1, <https://bitcoin.org/bitcoin.pdf> (last visited Sept. 26, 2019). The legal implications of Internet disintermediation were explored two decades ago. Andrew L. Shapiro, *Digital Middlemen and the Architecture of Electronic Commerce*, 24 *OHIO N.U. L. REV.* 795, 795–812 (1998).

As yet, there is little rigorous writing on smart contracts,¹¹ but those few accounts generally agree upon three things. The first, and perhaps defining, feature of a smart contract is that it is *unbreakable*.¹² It not only self-operates (positive automation); it also precludes outside influence (negative automation).¹³ There is no need for a contracting party to trust their counterparty to perform, or any intermediary to secure performance. Performance is inevitable.

The second, related claim is that smart contracts are designed to be (and are in fact) *non-justiciable*.¹⁴ Commentators present this either as the idea that smart contracts admit no legal oversight at all,¹⁵ or as a matter of independent normative ecology; if there are rules that apply to smart contracts, no territorial State has a role in making and applying them.¹⁶ Thus, smart contracts are both “self-executing” and “self-enforcing.”¹⁷ These characteristics are usually

¹¹ The few articles include: Simon Geiregat, *Cryptocurrencies Are (Smart) Contracts*, 34 COMPUTER L. & SECURITY REV. 1144 (2018); Sarah Green, *Smart Contracts, Interpretation and Rectification*, LLOYD’S MAR. & COM. L.Q. 234 (2018); Jeffrey M. Lipshaw, *The Persistence of Dumb Contracts*, 2 STAN. J. BLOCKCHAIN L. & POL’Y 1 (2019); Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017); Alexander Savelyev, *Contract Law 2.0: ‘Smart’ Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COM. TECH. L. 116 (2017); Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2017); Werbach & Cornell, *supra* note 9; Michèle Finck, *Smart Contracts as a Form of Solely Automated Processing Under the GDPR*, 2 (Jan. 8, 2019) (Max Planck Institute for Innovation and Competition Research Paper No. 19-01); Gabriel Olivier Benjamin Jaccard, *Smart Contracts and the Role of Law*, JUSLETTER I.T. 23 § 3 (Nov. 2017); *see also* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, (Mar. 12, 2015) (unpublished) (available at https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf).

¹² Werbach & Cornell, *supra* note 9, at 318 (Smart contracts “eliminate the act of remediation, by admitting no possibility of breach.” The only input required is the single trigger event.).

¹³ Beyond the trigger event, positive automation is the ability to operate without outside input; negative automation precludes such input.

¹⁴ Wright & De Filippi, *supra* note 11, at 50 (arguing that this requires “at a minimum a redefinition of how laws and regulations are designed, implemented, and enforced”).

¹⁵ *See, e.g.*, Werbach & Cornell, *supra* note 9, at 350 (smart contracts “supersede legal enforcement”).

¹⁶ *See generally* Vili Lehdonvirta, *The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy*, OXFORD INTERNET INST. (Nov. 21, 2016), <https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/>.

¹⁷ Werbach & Cornell, *supra* note 9, at 320. I have called the “self-executing” nature of smart contracts negative automation: the point is not just that they operate without input, but that they preclude operational input. *See also* KEVIN WERBACH, *THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST* 64 (2018) (“[F]or all practical purposes, the machine is the entirety of the contractual environment. It needs no human intervention, either to perform the contract or to resolve disputes in court.”).

attributed to the technology that underpins the cryptocurrency “Bitcoin,” called “blockchain technology.”¹⁸

The final point of consensus is that this is a *good thing*—for business certainly, but for consumers, too. For some, the potential is almost limitless: smart contracting will “transform law, finance, and civil society.”¹⁹ For others, the message is subtler: smart contracting represents the “mature end of the evolution of electronic agreements over several decades.”²⁰ But most agree that, by limiting intermediation and operational interference, smart contracts enhance efficiency, transparency, and granular control.²¹

The vision that emerges from these three claims is both utopian and classically liberal. Parties can digitize and automate contracts in such a way as to immunize performance from interference in tempore²² and ex post.²³ They can, in this sense, transact within a domain free from State supervision.²⁴

The claims are easy to recite, but harder to illustrate. Commentators use a familiar archetype: just as a vending machine collects payment and (usually) delivers the chosen item in an observable, tamper-proof way, “smart contracting” describes the automated delivery of *digital* assets.²⁵ Smart contracts are, in this

¹⁸ WERBACH, *supra* note 17 (“[S]mart contracts turn a distributed ledger into a distributed computer.”); Gideon Greenspan, *Beware the Impossible Smart Contract: The Three Most Common Smart Contract Misconceptions*, MULTICHAIN (Apr. 12, 2016), <https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract/> (“A smart contract is a piece of code which is stored on a blockchain, triggered by blockchain transactions, and which reads and writes data in that blockchain’s database.”); Jaccard, *supra* note 11; Sklaroff, *supra* note 11, at 273 (“agreements built in computer code and stored on a blockchain”).

¹⁹ 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 (Mar. 19, 2015, 12:10 PM), <http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn>; see also Wright & De Filippi, *supra* note 11, at 3 (“The blockchain has the potential to usher in a new era characterized by global payment systems, digital assets, decentralized governance, and even decentralized legal systems.”).

²⁰ Werbach & Cornell, *supra* note 9, at 317.

²¹ *Id.*

²² Green, *supra* note 11, at 234 (Smart contracts are “self-executing agreements”; they cannot be interrupted by the parties themselves or third parties.).

²³ Savelyev, *supra* note 11, at 127 (“Smart contract [sic] does not need any legal institutions to exist.”).

²⁴ This echoes claims made in the early years of the Internet. LESSIG, *supra* note 4, at 3–8.

²⁵ This was the example that Szabo employed in his 1997 blog post. *Smart Contracts*, *supra* note 7. Szabo envisaged that smart contracts would transcend the vending machine, allowing users to “embed contracts in all sorts of property that is valuable and controlled by digital means.” *Id.* This is now the “go-to” example for commentators. See, e.g., WERBACH, *supra* note 17, at 64–65 (“[V]ending machines work as proto-smart contracts because they sell items of low value, operate face to face, and take cash. . . . Distributed ledgers make it possible to implement similar arrangements digitally, across networks, for any kind of asset or agreement, without any trusted actor.”).

sense, a sort of “virtual vending machine.”²⁶ And it is generally understood that all of this was made possible by the advent of blockchain technology in 2008.²⁷ Yet, fundamental questions remain unanswered: Are smart contracts a type of a computer code,²⁸ a type of contract,²⁹ or both?³⁰ Which tasks can only be accomplished, or can be accomplished more easily, using smart contracts? Precisely what role does blockchain technology play? Without answers to these questions, it is impossible to offer a robust critique of the practice of smart contracting. Accordingly, this Article has two goals that are—in light of the paucity of academic literature—equally important. The first is descriptive: I explain what “smart contracts” are, and how they differ from the commercial tools that we already have. The second is normative: I consider whether smart contracting offers, on balance, a better way of facilitating valuable commitments.

I address the explanatory task in Part II. The purpose of smart contracting, I show, is to make contractual performance tamper-proof. This is where Bitcoin comes in. By crowdsourcing³¹ the task of transferring an asset from A to B,³² blockchain technology ensures that no single person controls or

²⁶ Sklaroff, *supra* note 11, at 271 (a “virtual machine”).

²⁷ So that there is a relationship of causal and material equivalence between these two tools. I call the protocols that support blockchain technology “blind consensus protocols.” *See infra* notes 84–106 and accompanying text. Blockchain technology, as we will see, provides a mechanism for persuading disparate actors to come to a dynamic consensus about a particular distribution of holdings, without the visible anchor of physical control.

²⁸ *See, e.g.*, James Grimmelmann, *All Smart Contracts Are Ambiguous*, PA. J.L. & INNOVATION (forthcoming 2019) (manuscript at 2); *A Primer on Smart Contracts*, U.S. COMMODITY FUTURES TRADING COMMISSION (Nov. 27, 2018), at 4, https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf (“a set of coded computer functions”).

²⁹ *See, e.g.*, THE RULE OF CODE, *supra* note 8, at 72–88 (distinguishing between smart contracts as legal agreements, and “smart contract code”); *see also* Geiregat, *supra* note 11; Wright & De Filippi, *supra* note 11, at 10–11 (“digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention”).

³⁰ *See, e.g.*, Werbach & Cornell, *supra* note 9, at 341–42.

³¹ Crowdsourcing is “the practice of obtaining information or services by soliciting input from a large number of people, typically via the internet and often without offering compensation.” *Crowdsourcing*, OXFORD ENG. DICTIONARY, <http://www.oed.com/view/Entry/376403#eid288590739> (last visited Sept. 26, 2019).

³² *See* Vitalik Buterin, *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform*, ETHEREUM, at 4, http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (last visited Sept. 30, 2019) (describing Bitcoin as a system for “decentralized consensus” as to who owns what); *see also* Wright & De Filippi, *supra* note 11, at 5 (“Prior to the invention of the blockchain, it simply was not possible to coordinate individual activities over the Internet without a centralized body ensuring that no one has tampered with the data.”).

can frustrate performance.³³ I complete Part II with two key distinctions—between computer code and contract, and between positive and negative automation. While the term “smart contract” has been used in a variety of ways, its “core case” is not a legal contract, but rather a type of code. A smart contract is computer code that negatively automates contractual performance.³⁴

With this picture in mind, I turn in Part III to the justificatory task. I show that, while negative automation guarantees counter-performance, it also has two significant downsides: it exposes parties to a greater risk of fraud and malicious hacking and makes it almost impossible for parties to avoid the impact of contracts that suffer from some serious defect in formative consent.³⁵ And this, I argue, counts—plainly and weightily—against the claim to consumer empowerment.

The law of contract strikes a careful balance between encouraging parties to abide by their promises and allowing parties to escape from ill-formed contracts.³⁶ In so doing, it supports and protects valuable relationships of trust and cooperation. The lesson taught by this experiment of contractual technology is simple but crucial: rather than trying to *rid* commerce of these relationships of trust, we should foster the transparency and accountability that they need to flourish.

II. EXPLAINING “SMART CONTRACTS”

In 1994, Nick Szabo introduced the idea of a “smart contract.”³⁷ For Szabo, this meant any “computerized transaction protocol that executes the terms

³³ This is the idea that I have called “negative-automation”: by placing operational control outside of the hands of any one person, blockchain technology makes it exceedingly difficult to impede performance. I deal with the practical methods by which the Bitcoin Blockchain is made secure below. *Infra* notes 103–106 and accompanying text.

³⁴ We will see that the term “smart contract” is used primarily by those who engage in the Ethereum community to describe a type of code. *Ethereum Homestead Documentation*, ETHEREUM, Mar. 1, 2017, at 71, <https://buildmedia.readthedocs.org/media/pdf/ethereum-homestead/latest/ethereum-homestead.pdf> (“A contract is a collection of code (its functions) and data (its state) that resides at a specific address on the 34343434 blockchain.”).

³⁵ On account of fraud, unconscionability, mistake, or some other unfair contract term produced by a substantial imbalance in bargaining power. This problem is particularly acute for those who are vulnerable, ill-informed, or who otherwise hold a bargaining position of relative impotence.

³⁶ In October 2018, Lord Hodge of the UK Supreme Court noted the importance of making sure that technological innovation did not override the subtle ways in which the law might assist those whose intent had been “vitiated.” *Financial Technology: Opportunities and Challenges to Law and Regulation*, SUP. CT., Oct. 26, 2018, at 14, <https://www.supremecourt.uk/docs/speech-181026.pdf>.

³⁷ *Smart Contracts*, *supra* note 7.

of a contract.”³⁸ The basic idea was that “many kinds of contractual clauses . . . can be embedded in the hardware and software we deal with” in such a way as to “proactively enforce” performance.³⁹ Szabo’s goals were twofold—to increase transparency (“the ability of the [parties] to observe each others’ [sic] performance of the contract”),⁴⁰ and to improve accountability (to “focus responsibility for the consequences of contract-related activity onto the parties”).⁴¹

Little in this is unorthodox or new.⁴² Any program that automates access to a particular service—whether infrastructure,⁴³ educational or recreational media,⁴⁴ or some other aspect of ordinary life—uses computer code to execute a legal contract. We interact with these programs often, and the advantages and disadvantages are reasonably well understood.⁴⁵ Yet, in all of these examples, access to the relevant service depends upon the continued cooperation of the service-provider; that service-provider provides the practical transactional infrastructure and retains the ability to alter or impede contractual performance. And here, Szabo hinted at a more disruptive vision—a way of taking counter performance *out* of the control of one’s counterparty or any other actor,⁴⁶ thereby placing control *back* in the hands of the service-user.

Szabo chose to exemplify this vision by way of a “canonical real-life example”: the “humble vending machine . . . takes in coins, and via a simple mechanism . . . dispense [sic] change and product according to the displayed price.”⁴⁷ The point of Szabo’s analogy was this: by setting up contractual exchange to self-operate in a way that precludes interference,⁴⁸ the vending

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² Even in 1994, when Szabo was writing.

⁴³ For example, contactless payment for public transport.

⁴⁴ For example, paying to access an online newspaper.

⁴⁵ Lessig’s treatise is comprehensive in its treatment of ethical risks. *See generally* LESSIG, *supra* note 4. Jaron Lanier weaves a compelling case for introducing better systems for permitting individuals to retain control over their data. *See generally* JARON LANIER, WHO OWNS THE FUTURE (2014); JARON LANIER, YOU ARE NOT A GADGET: A MANIFESTO (2011). For a directly political approach, *see generally* JAMIE BARTLETT, THE DARK NET: INSIDE THE DIGITAL UNDERWORLD (2015) [hereinafter BARTLETT, THE DARK NET]; JAMIE BARTLETT, THE PEOPLE VS TECH: HOW THE INTERNET IS KILLING DEMOCRACY (AND HOW WE SAVE IT) (2018) [hereinafter BARTLETT, THE PEOPLE VS TECH].

⁴⁶ Whether intermediary or counterparty.

⁴⁷ *Smart Contracts*, *supra* note 7.

⁴⁸ *Supra* note 13 and accompanying text. This is what I have called negative automation.

machine guarantees counter performance. Buyers do not need to place their trust in any counterparty or intermediary. They may simply trust *machines*.⁴⁹

For Szabo, the idea of a “smart contract” went beyond the vending machine “in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means.”⁵⁰ He exemplified this idea by way of an instalment plan:⁵¹ the buyer receives a car in return for a promise to pay the price in stages, and a smart contract transfers the car’s e-key to the owner automatically if the buyer defaults. This arrangement, he said, would be “much cheaper and more effective than a repo man,” would provide “better observation and verification,” and better transactional security.⁵²

The cryptocurrency known as “Bitcoin” was part of the machinery that would facilitate Szabo’s vision of secure, peer-to-peer transactions in the digital realm.⁵³ That platform, first described in 2008⁵⁴ and launched in 2009,⁵⁵ created a mechanism for transferring digital coins without relying upon the infrastructure of traditional financial intermediaries. Parties could now transfer digital assets without banks and payment providers, on a peer-to-peer basis. Though limited to one particular digital asset (“bitcoins”), the underlying technology (“blockchain technology”) encompassed a set of tools that could be used for many different kinds of digital assets.⁵⁶

In the wake of the 2017 Bitcoin “Gold Rush,”⁵⁷ Szabo’s ideas made their way into mainstream academic literature. Szabo’s core case (the “humble vending machine”) became prototypical, and his task of generalization was taken up with zeal. As of 2019, blockchain technology has been identified as a rich

⁴⁹ Sarah Green calls this “trustless” contracting. Green, *supra* note 11, at 236. Note, though, that it is not wholly so: the point is that, rather than trusting that an individual will behave as promised, the contracting party may trust the machine to perform the function that it has been set up to perform.

⁵⁰ *Smart Contracts*, *supra* note 7.

⁵¹ In the other common law countries, these arrangements are known as “hire purchase” arrangements. See, e.g., EWAN MCKENDRICK, *GOODE ON COMMERCIAL LAW* 296 (5th ed. 2016).

⁵² *Smart Contracts*, *supra* note 7.

⁵³ Werbach & Cornell, *supra* note 9, at 324. (“The development that made Szabo’s vision of smart contracts more than a mere curiosity was Bitcoin.”).

⁵⁴ See Nakamoto, *supra* note 10, at 4.

⁵⁵ This was the point at which the first open-source bitcoin client was created, and the first bitcoins “mined.”

⁵⁶ Kevin Werbach, *Trust, But Verify: Why Blockchain Needs the Law*, 33 *BERKELEY TECH. L.J.* 487, 518 (2018) (describing systems for “coloring” coins, by means of software that allocates information about another (real-world or digital) asset to transaction metadata). In what follows, we will consider other platforms that use the tools of Bitcoin to accommodate a variety of different structures for owning and transferring a variety of different assets.

⁵⁷ See, e.g., Olivier Huez, *Bitcoin Frenzy: 19th Century Gold Rush Lessons for Crypto-Mining*, MEDIUM (Dec. 30, 2017), <https://medium.com/c4-ventures/bitcoin-frenzy-19th-century-gold-rush-lessons-for-crypto-mining-4bfe10e163>.

field for negatively-automated transactions,⁵⁸ from land and corporate share registry,⁵⁹ to pornography⁶⁰ and seed-to-sale marijuana tracking.⁶¹ For all such applications, the promise is one of better efficiency, greater transparency, and a way of placing contractual control back in the hands of the individual consumer.

Yet, there is such a wide gap between the goals of technologists and lawyers that the same terms adopt starkly different meanings. “Contract” has proven particularly difficult. For legal commentators, the term describes a particular type of bilateral relationship.⁶² For computer scientists, the term describes a particular type of code.⁶³ Still, others prefer to view code and contract as a single device.⁶⁴ Moreover, there are many different claims about the way in which blockchain technology interacts with contractual automation.⁶⁵ To account for this variation, attempts to define “smart contracts” comprehensively have been almost comically broad: “A smart contract is an automatable and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code.”⁶⁶ These

⁵⁸ UK GOV’T CHIEF SCI. ADVISER, DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 21 (2016), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf/.

⁵⁹ *HM Land Registry to Explore the Benefits of Blockchain*, GOV.UK (Oct. 1, 2018), <https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain>.

⁶⁰ SpankChain, *Introducing CryptoTitties: An Onboarding and Educational Tool to Finally Give Titties Their Day on the Ethereum Blockchain*, MEDIUM (Feb. 9, 2018), <https://medium.com/spankchain/introducing-cryptotitties-2d0b2df1fca5>.

⁶¹ Brian Penny, *Blockchain Buds: Tracking Cannabis from Seed to Sale*, CRYPTO BRIEFING (Sept. 2, 2018, 11:02 AM), <https://cryptobriefing.com/cannabis-blockchain-seed-to-sale/>.

⁶² See, e.g., RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 1981) (“A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty.”); EDWIN PEEL, TREITEL ON THE LAW OF CONTRACT § 1–001 (13th ed. 2011) (“A contract is an agreement giving rise to obligations which are enforced or recognized by law.”).

⁶³ The best example of this usage is the Ethereum Homestead Documentation. See, e.g., *Ethereum Homestead Documentation*, *supra* note 34 (“A contract is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.”).

⁶⁴ Werbach & Cornell, *supra* note 9, at 341–42. They call smart contracts a “chunk of code,” but conclude that “smart contracts are, at the conceptual level, still contracts.” *Id.* at 342.

⁶⁵ For most, blockchain technology is a necessary prerequisite to smart contracts, but others seek to keep the two conceptually distinct. See, e.g., Christopher D. Clack et al., *Smart Contract Templates: Foundations, Design Landscape and Research Directions*, BARCLAYS BANK PLC, Mar. 15, 2017, at 2, <https://arxiv.org/pdf/1608.00771.pdf>; Raskin, *supra* note 11, at 306 (Smart contracts are “agreements wherein execution is automated, usually by computers.”).

⁶⁶ Clack et al., *supra* note 65 (calling this a “higher-level definition based on the two topics of automation and enforceability”). These two topics are smart contracts as a legal contract and smart contracts as code. *Id.*

problems are not superficial or merely semantic. There is now a wide divergence in substantive claims about the nature and impact of smart contracting,⁶⁷ and the relationship that it bears to blockchain technology and the established law of contract.⁶⁸

It is long past time for a clear exposition of precisely how Szabo's vision has come to be translated into a set of practical tools for digital commerce. The goal of Part II of this article is to develop such an account. The goal of Part III is to use that account to assess the merits of smart contracts.

A. *Automating Asset-Sales: Creating Confidence in Counter Performance by Limiting the Power for Intervention*

In what follows, I explain what Szabo was asking us to imagine in 1994, and why—25 years ago—it was what one might appropriately call “visionary.” Through a step-by-step progression from real-world asset sales to automated digital asset sales, I demonstrate what we need to build Szabo's virtual vending machine. The missing pieces of our commercial toolbox, I show, are: first, some method for transferring digital assets directly from one person to another; and second, a way of stopping sellers from altering or frustrating contractual performance.

1. Buying and Selling Assets

In order to enter into an agreement for the sale of an asset (“X”), both buyer (“B”) and seller (“S”) need to be satisfied of (at least) three things. First, they must have *consensus* on material aspects of the sale: the parties must identify X, the price (“P”), and how sale is to occur. Second, each party must be sufficiently confident of *counter performance*. Wherever there is a way of interrupting performance, this requires an element of trust. Each party must hope

⁶⁷ See Wright & De Filippi, *supra* note 11, at 2–3 (claiming that “[w]e stand at the edge of a new digital revolution” and that “the blockchain has the possibility to fundamentally change the way people organize their affairs”). But see Kai Stinchcombe, *Ten Years In, Nobody Has Come Up with a Use for Blockchain*, CNBC (Dec. 26, 2017, 10:30 AM), <https://www.cnbc.com/2017/12/26/ten-years-in-nobody-has-come-up-with-a-use-for-blockchain.html> [hereinafter Stinchcombe, *Ten Years In*]; Kai Stinchcombe, *Blockchain Is Not Only Crappy Technology But a Bad Vision for the Future*, MEDIUM (Apr. 5, 2018), <https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-a-medieval-hellhole-clca122efdec> [hereinafter Stinchcombe, *Blockchain*] (arguing that “[t]here is no single person in existence who had a problem they wanted to solve, discovered that an available blockchain solution was the best way to solve it, and therefore became a blockchain enthusiast”).

⁶⁸ Green, *supra* note 11, at 235 (arguing that smart contracting *supplements* the law of contract: “computers can now also be used to carry out the entire contractual process, from formation to execution”); Werbach & Cornell, *supra* note 9, at 363 (arguing that smart contracting exists in an “orthogonal” relationship with the law of contract).

that the other will make good on their promise when the time for performance arrives. Finally, each party must be sufficiently confident that, post-sale, the rest of the world will behave as if B and S are entitled to *X* and *P* respectively. This is usually termed *security of receipt*, though the idea is more specific than continuing physical possession. It describes a successful change in the identity of the person treated as entitled to deal with the relevant asset.⁶⁹

The amount of reassurance B and S require at each stage varies according to factors that include the type of asset, the value of *X*, and the conditions of sale. Take the following Example 1.1:

Example 1.1: S owns and runs a convenience store. Soda is advertised for sale at a price of \$1/can. B selects a can, hands \$1 to S at the counter, and exits the store with the drink.

In this example, consensus is reached through the price-label, and the unarticulated terms incorporated by ordinary practice.⁷⁰ Confidence in counter performance comes from various sources—for B, physical possession of the can and the store's reputation,⁷¹ for each the possibility of legal recourse. The sources of confidence in security of receipt overlap: possession, reputation, the paper receipt, the physical parameters of the cash register, and the legal system that underpins the contractual relationship. But by and large, neither party will examine the circumstances of sale too hard. Because of the low value of the goods and consideration, each is prepared to accept some risk.

Variations in the conditions of sale may, however, make the parties less relaxed. If the store is located in an area in which petty crime rates are high, S may decide to install surveillance equipment or employ security personnel. If the asset is worth substantially more than \$1, both parties are likely to require more by way of reassurance.⁷² For certain assets, those cautionary steps are mandated by law. The sale of a house, for instance, requires a deed of conveyance and registration.

So, buyer and seller must agree upon some basic terms of sale and must be confident that they can expect undisturbed possession (of the asset or its price) after sale has taken place. The events necessary to generate that confidence vary by context.

⁶⁹ Or, more precisely, the person entitled to set the parameters for who is allowed to interact with that asset.

⁷⁰ For example, that the price label refers to any one of the described categories, the buyer can obtain delivery immediately, etc.

⁷¹ Or the reputation of similar shops.

⁷² Those who purchase cars through eBay auctions will only part with money once they are assured of physical possession and may require additional proof of no rival claims (by way of the handbook and registration certificate).

2. Automating Asset Sales

There is an old and simple mechanism by which the buyer may gain *absolute* confidence in counter performance:

Example 1.2: S has a roadside stall, offering soda for sale at a price of \$1/can. S puts out a tin to collect payment and leaves the stall unmanned. B selects a can, puts \$1 in the collection tin, and leaves with the drink.

There are obvious advantages to such a setup. B can simply take possession, without the need for S (or S's agent) to be present. In a sense, these are the "smartest" contracts around; sale can occur by self-help, without the need for any machine.

But B's additional confidence in counter performance comes at a price to S. S no longer has any assurance that B will perform. S must simply trust the good intentions of any would-be customer. Accordingly, these transactions work for low-value, low-frequency sales, but they do not give us a blueprint that works at scale. And thus, we arrive at the impetus for secure, automated contract performance—a way of providing *mutual* assurance that each party will perform.

The mechanical answer to that demand has a surprisingly long pedigree. Hero, a first century A.D. Greek engineer and prolific inventor, documented the first-known vending machine in his text *Mechanics and Optics*.⁷³ Hero's machine accepted a five Drachma coin, which would push a platform down, opening a valve and dispensing a trickle of water. The pan would continue to tilt with the weight of the coin until it fell off, at which point a counter-weight would push the lever back up and turn off the valve. This is an ancient precursor to the modern snack-dispenser, and it provides a (relatively) cheap and easy mechanism for securing the counter performance of *both* parties, while protecting the money price from interference.

Modern vending machine transactions operate as follows:

Example 1.3: S owns and stocks a vending machine, in which soda is offered for sale at a price of \$1/can. B selects a can, puts coins of the correct value in the slot, and recovers the drink from a tray at the base.

Szabo described the vending machine as "a contract with bearer."⁷⁴ Yet, it is worth emphasizing here, because it will be crucial later,⁷⁵ that the contractual process occurs in the *background* to the mechanical operation. The vending machine owner (S) makes an open offer in the form "If you pay me \$1, I will give you a can of soda of the kind that you have selected." By putting coins into

⁷³ See generally VICTOR J. KATZ, A HISTORY OF MATHEMATICS: AN INTRODUCTION (1998).

⁷⁴ *Smart Contracts*, *supra* note 7.

⁷⁵ See *infra* Section II.A.1.

the slot, B accepts that offer and imposes a duty on S to deliver the drink. That obligation is executed by the vending machine. In short, the vending machine is not *itself* a contract; it executes a contract. From the perspective of the law, therefore, there is very little difference between a vending machine and a roadside stall. The practical difference between them lies in the mode of performance—by self-help on one hand, by mechanized delivery on the other.

Thus, the vending machine does what the roadside stall cannot: it provides confidence in counter performance for *both* parties. Each can simply trust the machine to deliver possession of the goods and price respectively.

3. Buying and Selling Digital Assets

We have already seen that the transfer of physical possession is usually enough to guarantee security of receipt. That simple feature facilitates a system of peer-to-peer commerce. Parties are content to deal directly with one another, without recourse to any other authority. But we cannot rely upon that mechanism in the digital realm. The reason for this is not (or not merely) that digital assets are intangible;⁷⁶ rather, it is that they are “non-rivalrous.”⁷⁷ Unlike the transfer of a coin or can, the transfer of digital information (“data”) does not entail relinquishing the object of transfer. Instead, it causes the information to be *replicated*. After the transfer, the transferor and the transferee will each hold a copy of the data. So, if we want data to behave like a real-world asset transfer—which is to say, if we want it to be possible to associate data with only *one* person—we have an additional obstacle. Take the following example:

Example 1.4: S owns and runs a convenience store. Soda is advertised for sale at a price of \$1. B selects a can and offers to pay with a digital coin.

In order to give S confidence that, post-sale, the world will behave as if S is the person properly entitled to spend that digital coin, we need some way of making sure that B will not subsequently draw upon the coin’s purchasing power. This is usually termed “double-spending,”⁷⁸ but the problem is not unique to money

⁷⁶ Note that digital data does have a physical presence. Rolf Landauer, *Information Is Physical*, 44 PHYSICS TODAY 23, 23 (1991) (“Computation is inevitably done with real physical degrees of freedom, obeying the laws of physics, and using parts available in our actual physical universe.”). See generally JAMES GLEICK, *THE INFORMATION: A HISTORY, A THEORY, A FLOOD* (2012). A legal interest, being a relationship between individuals to which the law affords a particular status, is intangible. A series of “0” or “1” states on computer storage components, held locally or provided by a server, is not: each memory cell is set to a high or low voltage level to reflect a “bit” of binary information. *Id.* at 204–33.

⁷⁷ See generally SARAH GREEN & JOHN RANDALL, *THE TORT OF CONVERSION* (2009).

⁷⁸ Nakamoto, *supra* note 10. See, e.g., THE RULE OF CODE, *supra* note 8, at 19–20; David Chaum, *Achieving Electronic Privacy*, 267 SCI. AM. 96, 97 (Aug. 1992); Green, *supra* note 11, at 236.

or to the digital realm. It exists on the same scale as the problem of “security of receipt” that we met in relation to Example 1.1 above.⁷⁹ The problem is not created, but rather exacerbated, by data.

The simplest solution to this problem is a centralized one, and it is one that we have already met.⁸⁰ We rely upon mutually-trusted third parties to tell us who owns what: registrars record entitlement to houses and to digital assets like domain names; for digital money transfers, we rely upon banks to execute payments and to provide information to their customers about account balances.

So, digital assets create an acute problem of confidence in security of receipt; that problem is usually solved by mutually-trusted third parties.

4. Automating Digital Asset Sales

Szabo’s goal was to extend the idea of automatic asset sales to the digital realm—to “embed contracts in all sorts of property that is valuable and controlled by digital means.”⁸¹ The first step towards that goal is simply to automate digital asset sales. This requires some way of manifesting assets digitally and programming computers to respond to pre-defined trigger events.⁸² These sorts of programs existed prior to 1994 and are now commonplace:

Example 2.1: S advertises e-books for sale online. *A Brief History of Time*⁸³ is offered for sale at a price of \$10. B clicks “buy,” effects payment, and downloads the book to an e-reader.

Access is granted automatically. Once paid for, the book can be downloaded without any further action on the part of S.

There are, however, two important differences between this sort of digital automation and our Example 1.3:

Example 1.3: S owns and stocks a vending machine, in which soda is offered for sale at a price of \$1/can. B selects a can, puts coins of the correct value in the slot, and recovers the drink from a tray at the base.

In Example 1.3, S cedes operational control to the vending machine. Because of this, B (assuming familiarity with the mechanism of sale) does not need to know or trust S. B simply trusts the machine. In Example 2.1, by contrast, S retains

⁷⁹ *Supra* Section II.A.1.

⁸⁰ *Id.*

⁸¹ *Smart Contracts*, *supra* note 7.

⁸² See generally Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629, 639 (2012) (A “data-oriented contract” is a contract “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.”).

⁸³ STEPHEN HAWKING, *A BRIEF HISTORY OF TIME: FROM THE BIG BANG TO BLACK HOLES* (1988).

operational control. And whenever S retains control, B must trust S that the program will operate as advertised.

Second, the sale in Example 1.3 can be executed without the help of any intermediary at the point of purchase.⁸⁴ Cash is a particularly clever technology, which permits peer-to-peer payment by physical delivery. Coins represent a credit balance that the holder can transfer by way of discharge of a payment obligation.⁸⁵ And, once triggered by payment, the machine will deliver the drink automatically. By contrast, B in Example 2.1 must rely upon a bank to effect payment,⁸⁶ and S must rely upon another bank to receive it.⁸⁷

Szabo proposed a way of dealing with these differences. By asking the reader to imagine the digital manifestation of a vending machine,⁸⁸ Szabo sketched out his vision of peer-to-peer transactions between untrusted actors in public networks. In the course of his 1994⁸⁹ and 1997⁹⁰ blog posts, Szabo identified some of the economic and technological devices that he thought would help to build his virtual vending machine.⁹¹ Yet, it was not until 2008 that these parts were assembled in such a fashion as to realize Szabo's vision *in toto*.⁹²

B. *Blind Consensus Protocols: Understanding the Political Model and Practical Ramifications of Blockchain Technology*

It is widely understood that Szabo's "virtual vending machine" was made possible by the technology, called "blockchain technology," that underpins the cryptocurrency "Bitcoin."⁹³ The term "smart contract" is now rarely used *without* a reference to blockchain technology.⁹⁴ There is, however, a great deal

⁸⁴ Prior to the point of purchase, sellers will usually rely on third parties to stock the machine.

⁸⁵ See generally Felix Martin, *Bitcoin Is Pointless as a Currency but It Could Change the World Anyway*, WIRED (Mar. 31, 2014, 6:30 AM), <https://www.wired.com/2014/03/bitcoin-currency-martin/>.

⁸⁶ And usually other intermediate payment providers as well.

⁸⁷ Or they may share the same bank.

⁸⁸ *Smart Contracts*, *supra* note 7.

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ Including digital signatures, public key encryption, and hierarchical transaction logs. *Id.*

⁹² See Nakamoto, *supra* note 10, at 4.

⁹³ Werbach & Cornell, *supra* note 9, at 324 ("The development that made Szabo's vision of smart contracts more than a mere curiosity was Bitcoin.").

⁹⁴ Smart contracts are described as "a piece of software code, implemented on a Blockchain platform, which ensures self-performance and the autonomous nature of its terms, triggered by conditions defined in advance and applied to Blockchain-titled assets." Savelyev, *supra* note 11, at 127; see also Michèle Finck, *supra* note 11, at 2 ("Smart contracts can be defined as self-executing code that automatically processes its inputs when it is triggered."); Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679, 680 (2019) ("[B]lockchain technology permits

of confusion about precisely how these two innovations relate to one another. For some, blockchain technology facilitates the manifestation of contractual agreement.⁹⁵ For others, it relates to the digital automation of contractual performance.⁹⁶ Yet, we saw above that it was possible both to manifest and automate contracts digitally prior to the advent of Bitcoin. What, then, does blockchain technology add? The answer, we will see, lies in the ability to generate enough confidence in counter performance and security of receipt to enable parties to transact on a peer-to-peer basis in the digital realm, just as they do offline.

We have seen that the anchor of possession is a powerful one. It allows parties to transact directly with one another, without resorting to third parties. We have also seen that data does not exhibit the traits necessary for such exclusive control; data is replicated, not relinquished, in the process of transfer. So far, therefore, parties contracting in the digital sphere have used intermediaries (banks, domain-name registrars, media companies, etc.) to tell them who owns what. Bitcoin facilitates the transfer of digital assets without these intermediaries. Its innovation is as much political as technological: Bitcoin encourages lots of actors to come to a consensus about the answer to the ownership question. In this way, Bitcoin allows parties to transact without using third parties, in a similar way to the peer-to-peer sale of real-world assets.

1. Blind Consensus

The basic elements of blockchain technology can be exemplified without recourse to the digital sphere. Imagine the following scenario:

“smart contracts” that allow coders to layer on top of currency exchanges particular conditions under which those exchanges will occur.”).

⁹⁵ See, e.g., THE RULE OF CODE, *supra* note 8, at 74 (“In many ways, smart contracts are no different than today’s written agreements.”); Green, *supra* note 11, at 235 (“[R]ather than using computers merely to *perform* pre-existing contractual agreements . . . computers can now also be used to carry out the entire contractual process, from formation to execution. This has been made possible by the advent of distributed ledger technology.”); Werbach & Cornell, *supra* note 9, at 368 (“A smart contract is computer code representing an agreement between two or more parties”); Mateja Durovic, *How to Resolve Smart Contract Disputes – Smart Arbitration as a Solution*, U. OXFORD FAC. L. (June 1, 2018), <https://www.law.ox.ac.uk/business-law-blog/blog/2018/06/law-and-autonomous-systems-series-how-resolve-smart-contract-disputes> (“[S]mart contracts require redress mechanisms that enable resolution of disputes without the need to leave the digital world.”); *Smart Contracts*, *supra* note 7 (“The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we dealt with.”).

⁹⁶ See, e.g., Finck, *supra* note 11, at 2 (Smart contracts are “one form of automated data processing that promise to generate efficiency gains while powering new markets and ventures.”); *Smart Contracts*, *supra* note 7 (“A smart contract is a computerized transaction protocol that executes the terms of a contract.”).

Scenario A: There are five prisoners—A, B, C, D and E. A is given a cell phone, and then all the prisoners are locked in separate rooms. Each room contains seven buttons: five represent the prisoners; two are simply marked ✓ and ✕. Any time one prisoner wishes to transfer the cell phone to another, that prisoner presses one of the identity buttons (A, B, C, D or E). Matching buttons light up in all the other rooms, and the other prisoners may press ✓ or ✕, thereby voting to approve or reject the transfer. If the would-be transferor does indeed have the phone, and other prisoners vote to approve it, all five are rewarded. Any other combination will see them all punished.

Let us assume that the prisoners are unrelated and have no history of dealings prior to their imprisonment. None has any reason to consider the others trustworthy—quite the opposite. Moreover, none can actually *see* who has the cell phone at any moment in time. In this sense, they are all operating “blind.” Nevertheless, three factors combine to give each a good reason to believe that the other inmates will vote, as a collective, to validate a transfer that meets the stipulations. First, each can infer the correct answer either from the original allocation to A, or from a previous transfer. Second, the method of communication is reliable. Finally, each is incentivized to vote honestly by the promise of reward and the threat of punishment. We now have a template for reaching “blind consensus”—a system for validating asset-transfers without resorting to third parties, in circumstances that preclude the visual identification of entitlement.

Instead of real-world assets, let us now assume a particular distribution of digital holdings. And instead of a single asset-transfer, let us assume that each of our participants can make transfers and receive assets, so that we need a more sophisticated mechanism for keeping track of transactions:

Scenario B: Anyone can buy, hold and transfer JailCoins. All participants in the JailCoin system have access to a chronological record of all previous transactions. Each can run a program that will tell them, by cross-checking that record, whether an individual has sufficient funds to make a particular transfer. Each also has access to an online forum. If one participant (“A”) wishes to transfer one JailCoin to another participant (“B”), A will indicate that intention on the forum. Other participants can then check the record to see whether A has sufficient funds and can vote on whether the transfer should go ahead. If A has one JailCoin, and if they vote “yes,” the transfer is added to the record and all participants are entered into a lottery to win one JailCoin.

As in Scenario A above, no participant can draw any visual cue from physical possession. But, as above, if there is a record of an earlier transaction in which A received a particular quantity of JailCoins (and no later record of A giving

them away), it will be possible for the participants to conclude that A has the capacity to make the transfer.⁹⁷ And as above, they are incentivized to vote for it to go through.

In principle, this works well enough, and (we will see) it broadly reflects the way in which the Bitcoin protocol operates. But we now face a hurdle, which we did not face in Scenario A. In the digital world, voting power can be captured unilaterally by making multiple identities.⁹⁸ This creates a problem for a system that relies on voting: by proliferating identities, participants are able to weight voting power in favour of a particular outcome. Prior to Bitcoin, this was a substantial obstacle in the way of implementing a disintermediated platform for digital commerce.

In 2008, a writer (or group of writers) under the pen name “Satoshi Nakamoto” brought together a variety of technological and economic innovations to solve this problem.⁹⁹ The protocol they designed, called “Bitcoin,” disincentivized identity capture by requiring participants to commit computing resources to the process of validating transactions. This solution is known as “proof of work.”¹⁰⁰ In an open network, proof of work equates identity to processing power.¹⁰¹ So, the Bitcoin Blockchain operates as follows, where a “miner’s” chance of winning the competition is roughly equal to the proportion of the network’s computing power that they control:

Scenario C: Anyone can buy, hold and transfer bitcoins. All participants have access to a time-stamped¹⁰² ledger of all previous transactions (“the Blockchain”). A participant (“A”) who wishes to transfer funds to another participant (“B”) must announce that intention to the network. Any participant can check the Blockchain to see whether A has capacity to do so. New transactions cannot be verified and added to the

⁹⁷ Blindness as to the asset is dealt with by a ledger.

⁹⁸ This is called a “Sybil attack,” named after the subject of a case study of a woman diagnosed with dissociative identity disorder. FLORA RHETA SCHREIBER, *SYBIL* (1973); Buterin, *supra* note 32. See generally Michael Nielsen, *How the Bitcoin Protocol Actually Works*, DATA-DRIVEN INTELLIGENCE (Dec. 6, 2013), <http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/>.

⁹⁹ See Nakamoto, *supra* note 10, at 4.

¹⁰⁰ The solution provided by proof of work is hardly elegant but has proven to be effective:

While nodes with a large amount of computational power do have proportionately greater influence, coming up with more computational power than the entire network combined is much harder than simulating a million nodes. Despite the Bitcoin blockchain model’s crudeness and simplicity, it has proven to be good enough, and would over the next five years become the bedrock of over two hundred currencies and protocols around the world.

Buterin, *supra* note 32, at 4.

¹⁰¹ See generally Nielsen, *supra* note 98.

¹⁰² Entries are noted with their relative chronological position.

Blockchain without the solution to a mathematical problem, which “miners” compete to solve. Once the answer is found, A’s transaction can be assigned to a group (“block”) of transactions and added to the Blockchain. The miner who solves the problem first receives one bitcoin.

In this way, parties may send and receive assets on a peer-to-peer basis, without the need for banks and other financial intermediaries. Like the JailCoin model, Bitcoin miners are incentivized to verify transactions by the prospect of receiving an economic reward (฿1).

The practical robustness of Bitcoin is secured by providing a workable solution to two related problems. The first is the need to choose between competing instructions to transfer a particular quantity of bitcoin. If A simultaneously instructs the network to transfer one bitcoin (called an unspent output, or “UTXO”) to B, and the *same* UTXO to another wallet that A controls, only one transaction will be added to the Blockchain. Whichever transaction is confirmed first by the miners will be processed. Thus, Bitcoin is often described as a “first to file” system.¹⁰³

The second problem is the need to thwart any attempt to reverse a transaction that has already been confirmed. Let us suppose that A instructs the network to transfer a particular UTXO to B and then seeks to reclaim it.¹⁰⁴ That transaction will be rejected by the miners, who can check the ledger and see that that output has already been spent. In order for A’s ploy to succeed, A will need to redo the mathematical problem that led to confirmation of the first transaction. This results in a “fork,”¹⁰⁵ producing two competing chains. Legitimate miners will continue to work on the original chain, leaving A’s chain redundant. In order to persuade the rest of the miners to work on A’s chain, A will need more computational power than the rest of the network combined.¹⁰⁶ For so long as fifty percent of that power lies with honest miners, A’s attack will fail.

These mechanisms immunize Bitcoin from attacks that would undermine the integrity of the platform as a whole. A person who receives bitcoin, just like a person who receives a coin or can of soda, can be reasonably confident that no one will come along and assert a superior claim. Thus, Bitcoin offers a practically-robust mechanism for transferring digital assets on a peer-to-peer basis—without banks and other financial intermediaries.

¹⁰³ See Buterin, *supra* note 32, at 1.

¹⁰⁴ To enable A to engage in what we have called “double-spending.”

¹⁰⁵ See Buterin, *supra* note 32, at 8.

¹⁰⁶ *Id.*

2. Crypto-Assets and Block-Chains

Above, I indicated that “bitcoins” are described as unspent transactional outputs (“UTXO”).¹⁰⁷ This is not a linguistic quirk; rather, it describes a substantive quality of the relationship between a user and “their” bitcoin. When a particular wallet holds “฿1,” that means that the wallet contains one or more UTXO totalling ฿1.¹⁰⁸ An instruction to transfer “a bitcoin” is an instruction to send one or more UTXO’s worth ฿1 (or more, returning change). No single “bitcoin” has a constant identity. Each is simply made up from the history of transactions by which one or more UTXO’s have come to be associated with a particular wallet address.¹⁰⁹ So, each bitcoin is unique, but none retains precisely the same form before and after a wallet transaction.¹¹⁰

The strength of the association with money makes it important to emphasize that the Blockchain is a record of who controls how much of a particular *thing*, rather than a record of the amount owed. Unlike other money media, Bitcoin it is not a credit network.¹¹¹ That is what makes it so easy to make the intellectual and practical leap from Bitcoin to protocols that host all sorts of other assets.¹¹²

¹⁰⁷ Not all blind consensus protocols are of this form: Ethereum relies on a “virtual computer” model. *See generally Ethereum Homestead Documentation*, *supra* note 34.

¹⁰⁸ Knut Karnapp, *What Do You Legally Own with Bitcoin?*, MEDIUM (Nov. 23, 2018), <https://medium.com/coinmonks/what-do-you-legally-own-with-bitcoin-97b083ed6a04> (describing the “power of disposition” that a private key offers over UTXO, and equating this to (a form of) legal ownership).

¹⁰⁹ *See Nielsen, supra* note 98 (“[I]n Bitcoin there’s not really any separate, persistent ‘coins’ at all, just a long series of transactions in the block chain.”).

¹¹⁰ Some of the best analogies, therefore, are with specific quantifies of oil or water: bitcoins are scarce, rivalrous, and fungible things, the physical constitution of which can change over time. The private key offers the control that one has over a particular UTXO. *See Preston Byrne, What Do You Legally “Own” with Bitcoin? A Short Introduction to Krypto-Property*, PRESTON BYRNE (Nov. 23, 2018), https://prestonbyrne.com/2018/11/23/krypto_property/.

¹¹¹ For money as a credit network, see A. Mitchell Inness, *The Credit Theory of Money*, 31 BANKING L.J. 151, 151 (1914); A. Mitchell Inness, *What Is Money?*, 30 BANKING L.J. 377, 377 (1913). This raises other questions about the nature of Bitcoin as a monetary asset, which I cannot consider in depth here. One point is worth making: insofar as the question is a functional one, if Bitcoin can in fact be used to discharge the payment liabilities through which we purchase things, it discharges one function of money (albeit, what might be described as a “private” money). It may, of course, turn out that those who hold and transfer Bitcoin do so with a different objective in mind; the absence of a monetary policy makes it difficult to maintain the sort of constant value that is necessary for the fluid circulation of an asset.

¹¹² Bitcoins themselves can be “colored,” by means of software that allocates information about another (real-world or digital) asset to transaction metadata. UK GOV’T CHIEF SCI. ADVISER, *supra* note 58, at 61. Blockchain technology provides a method that

opens up the possibility of money with more than just value: it could carry attributes such as necessary purpose, expiry date, or location of allowed use. For example, money may have restrictions on the kind of goods and service it

Two semantic points bear emphasis at the conclusion to this section. First, the term “blockchain” has come to mean a variety of things, not all of which reflect the features of protocols under consideration here. “Block-” literally describes the grouping of transactions, which is necessary to slow the rate of verification enough for participants to be able to see which chain should command their computational resources.¹¹³ It is *not* necessary in closed systems that do not rely upon proof of work.¹¹⁴ I have chosen the label “blind consensus protocol,” which serves our purposes better. It emphasises the ability to generate agreement about whether a participant has the resources to execute a particular transfer, without the visible anchor of physical possession. The set of rules that implements that solution is a “blind consensus protocol.” The transactional environment that implements those rules is a “blind consensus platform.”

Second, I have used the term “disintermediated.” The term is prolific, but it is not actually entirely accurate. Bitcoin’s process of transaction verification is distributed (anyone may in theory take part), but intermediated: miners are intermediaries.¹¹⁵ The ideological notion of absolute disintermediation stems from the idea that network users are also miners, so that there are not two distinct groups of actors—those who use the system in a fashion akin to ordinary consumers, and those who contribute to the system by verifying transactions. In practice, there *are* two distinct groups, with very little cross-over. Nevertheless, I will adopt the term “disintermediated” here, as it reflects the important idea that traditional intermediaries are absent from the process.

Above, I identified two features that set the vending machine apart from any ordinary automated asset-delivery program; first, confidence in counter performance does not depend upon the seller’s reputation; second, sale can be executed without the help of any intermediary at the point of purchase. For a small class of assets, at least, Bitcoin provides a way of eliminating the second difference. It allows parties to transact on a peer-to-peer basis, without the infrastructure of traditional intermediaries.

can be used to purchase . . . ; or someone renting a flat through Airbnb may have their electronic access key revoked if they fail to pay on time, or if their contract has expired.

Id. at 57. We will see in what follows that there now exists a platform that permits more nuanced structures of asset control and delivery, facilitating a richer system for transacting in public networks.

¹¹³ See Mike Hearn, *Corda: A Distributed Ledger*, CORDA, Nov. 29, 2016, at 30 https://docs.corda.net/_static/corda-technical-whitepaper.pdf.

¹¹⁴ *Id.*

¹¹⁵ This point is rarely made, but it is important: it raises questions about whether it is better to place trust in the operation of a *variety of* intermediaries (as well as the code architects), rather than one intermediary. These are not trust-free transactions. See Bruce Schneier, *There’s No Good Reason to Trust Blockchain Technology*, WIRED (Feb. 6, 2019, 9:00 AM), <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>.

C. *Smart Contracts: Negatively-Automated Asset Sales and the Digital Environment*

We have seen that contracts could be manifested and executed automatically prior to the creation of Bitcoin.¹¹⁶ The contribution of blind consensus protocols is to facilitate a specific *type* of digital transaction, which is the transfer of an asset on a peer-to-peer basis—without trusting any one actor (counterparty or intermediary).

This provides part but not all of the machinery that we need to get to our virtual vending machine. Let us return to Example 1.3:

Example 1.3: S owns and stocks a vending machine, in which soda is offered for sale at a price of \$1/can. B selects a can, puts coins of the correct value in the slot, and recovers the drink from a tray at the base.

The vending machine automates one side of a bilateral exchange. And it does so in circumstances that place performance outside S's control. Contractual performance is *negatively automated*. A vending machine not only self-operates; it also does so in a way that precludes interference with contractual performance. What we need to complete the analogy between vending machine sales and digital asset sales is some similar mechanism for combining automation with disintermediation so as to remove operational control from the seller. The outcome of that combination, we will see, is a "smart contract."

1. Putting It All Together: Negatively-Automated Asset Sales

The next step in our progression, from physical asset sales to negatively-automated digital asset sales, is to design a program that interacts with a blind consensus platform:

Example 2.2: An online newspaper accepts payment in Bitcoin. If a reader ("B") pays \$0.01, B is automatically granted a one-month subscription.

The contract is positively automated. Once triggered, the program executes the contract without any further human input. But that program remains within the control of the newspaper. It is possible for the newspaper to withdraw or otherwise interrupt the reader's access. And this is the crucial point, which distinguishes positive from negative automation. The vending machine not only delivers the asset without operational input; that transaction cannot easily be frustrated by any single actor, whether S or some third party. So, in order to make Example 2.2 look more like Example 1.3, we need a way of taking the *software*—the rails of the transaction—outside of S's control.

¹¹⁶ *Supra* Section II.A.4.

Bitcoin facilitates a basic version of this sort of enterprise. UTXO can be controlled by script (a particular type of code that instructs a program) that requires pre-designated data to unlock that output.¹¹⁷ That script then cannot be altered by any single actor. However, its transactional ecology is limited. There are very few ways in which individuals can set up automated transactions within Bitcoin's infrastructure.

The Ethereum platform, launched in 2015,¹¹⁸ was devised to remove these limitations. Termed a "programmable blockchain,"¹¹⁹ the purpose of Ethereum was to provide a more complete and complex language for building programs that could interact with digital assets on blind consensus platforms.¹²⁰ The Ethereum Foundation describes the project as "a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference."¹²¹

Ethereum allows parties to design their contract such that no single entity controls or can alter performance. Take the following example, where "cryptokitty" describes a particular on-platform asset (a collectible, digital cat)¹²² and "Ξ" denominates Ether, which is the currency of Ethereum:

Example 3.1: S offers a cryptokitty ("Kitty 572634") for sale for Ξ1. S also uploads script that, when triggered by payment, will cause the cryptokitty to be transferred to the buyer. B transfers Ξ1 and receives Kitty 572634.

In this example, the whole transaction—payment of the price and transfer of the asset—is governed by the blind consensus platform. The script cannot be altered once it has been uploaded to the platform, and S cannot prevent the transfer from occurring when B meets the stipulated condition.

We are now in a position to return to those features which set the vending machine apart from any ordinary automated asset-delivery program: B does not need to trust S, and sale can be executed entirely without the help of any intermediary at the point of purchase. Bitcoin removed the second difference (intermediation). By removing both differences within the same transactional environment, Ethereum completes the vending machine analogy. S and B may set up an asset-transfer that is positively automated (requires no operational input beyond the trigger event) and negatively automated (once uploaded, *precludes*

¹¹⁷ See generally Buterin, *supra* note 32.

¹¹⁸ *Id.*

¹¹⁹ See generally *What Is Ethereum?*, ETHEREUM HOMESTEAD, <https://ethereum-homestead.readthedocs.io/en/latest/introduction/what-is-ethereum.html> (last visited Oct. 6, 2019).

¹²⁰ See generally Buterin, *supra* note 32.

¹²¹ *What Is Ethereum?*, CONSENSYS, <https://consensys.net/knowledge-base/about-ethereum-eth/> (last visited Oct. 6, 2019).

¹²² See CRYPTOKITTIES, <https://www.cryptokitties.co> (last visited Oct. 10, 2019).

further input). S and B may now transact with mutual confidence in counter performance. They need not trust one another or any third party; they can simply trust the Ethereum platform. This, finally, is Szabo's virtual vending machine.

2. Digital Contracts for Public Networks

The vending machine is a useful analogy for the way in which goods move within public networks between unknown and untrusted actors. A defined range of goods can be offered for sale in a visible, automated way.¹²³ But Szabo imagined a rich contractual environment, in which parties could manipulate the conditions for asset-transfer in a multitude of different ways.¹²⁴ Ethereum allows parties to do just that. Its programming language is sufficiently flexible to permit the creation of a variety of different structures for owning and transferring assets, which can be designed in such a way as to govern those assets over extended periods of time. The "decentralized autonomous organisation" ("DAO")¹²⁵ is now a well-known (though much-maligned) vehicle for facilitating long-term financial decision-making:

Example 4: A set of interoperable scripts control digital wallets to which platform users may commit funds during a designated window. Those scripts are designed to direct a series of investments over a fixed period of time, paying any investment return to users in proportion to funds committed.

Moreover, scripts can be designed to interact with "oracles,"¹²⁶ which feed them information about the real-world:

Example 5: A and B bet on a horse race. If Piccolo Star wins the Kentucky Derby, $\Xi 1$ will be deducted from B's wallet and sent to A's wallet. If Piccolo Star does not win, $\Xi 0.1$ will be deducted

¹²³ Buterin defines a smart contract as "a mechanism involving digital assets and two or more parties, where some or all of the parties put assets in, and assets are automatically redistributed among those parties according to a formula based on certain data that is not known at the time the contract is initiated." Vitalik Buterin, *DAOs, DACs, DAs, and More: An Incomplete Terminology Guide*, ETHEREUM BLOG (May 6, 2014), <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>.

¹²⁴ *Smart Contracts*, *supra* note 7 ("Smart contracts combine protocols, users interfaces, and promises expressed via those interfaces, to formalize and secure relationships over public networks. This gives us new ways to formalize the digital relationships which are far more functional than their inanimate paper-based ancestors.").

¹²⁵ Wright and De Filippi describe this vehicle as follows: "These organizations can re-implement certain aspects of traditional corporate governance using software, enabling parties to obtain the benefits of formal corporate structures, while at the same time maintaining the flexibility and scale of informal online groups." Wright & De Filippi, *supra* note 11, at 3; *see also* Buterin, *supra* note 32.

¹²⁶ *See, e.g.*, THE RULE OF CODE, *supra* note 8, at 75.

from A's wallet and sent to B's wallet. An oracle feeds the information "Piccolo Star wins the Kentucky Derby," and $\Xi 1$ is sent from A to B.

In this way, Ethereum provides a platform for allowing parties to memorialize (suitable parts of) relatively sophisticated, interdependent contractual steps in code, rendering performance immune from outside interference.

3. Three Smart Contracts; One Core Case

Equipped with a better understanding of Szabo's objective and the tools with which that objective has been realized, we are now able to turn to the definitional task. Here, two crucial distinctions emerge from the literature. The first and most important is a distinction between code and contract. The second is a distinction between positive and negative automation.

For some, the term "smart contract" describes a legal contract that is implemented by a particular type of code.¹²⁷ For others, it describes a type of code that, when uploaded to a blind consensus platform, precludes operational interference.¹²⁸ Indeed, some in the latter camp now lament Szabo's use of the term "smart contract," preferring "persistent script."¹²⁹ The perpetuation of this ambiguity is hardly surprising: "contract" carries a great deal of linguistic baggage.¹³⁰ Yet, if it is not possible to find consensus in the literature that has been produced over the last two decades, it is possible to deduce Szabo's intended meaning. In those two seminal blog posts,¹³¹ Szabo described a

¹²⁷ See, e.g., CHRISTOPHER D. CLACK ET AL., SMART CONTRACT TEMPLATES: FOUNDATIONS, DESIGN LANDSCAPE AND RESEARCH DIRECTIONS 2 (last revised Mar. 15, 2017), <https://arxiv.org/pdf/1608.00771.pdf>. The term "smart contract" is used primarily by those who engage in the Ethereum community to describe a type of code. See generally *What Is a Contract?*, ETHERIUM HOMESTEAD, <https://ethereum-homestead.readthedocs.io/en/latest/contracts-and-transactions/contracts.html#writing-a-contract> (last visited Oct. 6, 2019) ("A contract is a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain."). In what follows, I show that Szabo uses the term to describe a narrower and more specific use of script, to codify contractual agreements.

¹²⁸ See, e.g., Jaccard, *supra* note 11, § 2 ("[W]e may roughly describe a smart contract as a computer code enforcing rules and consequences."). I assume here, *arguendo*, that there is a distinction to be drawn between code and contract; I address this distinction in Part III.

¹²⁹ Vitalik Buterin used this term in a tweet. He said, "To be clear, at this point I quite regret adopting the term 'smart contracts.' I should have called them something more boring and technical, perhaps something like 'persistent scripts.'" Vitalik Buterin (@VitalikButerin), TWITTER (Oct. 13, 2018, 10:21 AM), <https://twitter.com/vitalikbuterin/status/1051160932699770882?lang=en>.

¹³⁰ See generally Alvaro Gonzalez Rivas et al., *Smart Contracts and Their Identity Crisis*, in THIRTY NINTH INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS, SAN FRANCISCO 2018 (Feb. 2, 2019).

¹³¹ See *Smart Contracts*, *supra* note 7.

particular *mechanism* for enforcing legal contracts. A smart contract, he said, is a “computerized transaction protocol that *executes* the terms of a contract.”¹³² Thus, for Szabo, a smart contract was a type of code, not a legal contract.

Szabo’s focus was not, however, as broad as the label “persistent script” implies. For Szabo, a “smart contract” did not refer to *any* implementation of persistent script, but rather the mechanism by which a *legal agreement* could be negatively automated.¹³³ So, if persistent script describes negatively-automated code (which may or may not execute a legal contract), and legal contracts may be negatively automated through mechanisms other than persistent script,¹³⁴ Szabo’s “smart contract” describes the overlap between these two devices. A “smart contract” is code that negatively automates contractual performance:

Figure 1:

To avoid categorical confusion, I will refer to persistent script and negatively automated legal contracts directly by those names.

The second distinction concerns the type of automation involved in a particular transaction. We have seen that Szabo’s objective was to come up with a system in which contracts could be set up (like the vending machine) to self-operate in a way that precludes intervention (what I have called negative automation throughout this article). We saw in the first part of this article that these negatively automated contracts are supported by blind consensus protocols. Yet, for some, the term “smart contract” is broader than this core case, including so-called “distributed”¹³⁵ systems over which a small number of parties retain

¹³² *Id.* (emphasis added).

¹³³ *Id.* (“The basic idea behind smart contracts is that many kinds of contractual clauses . . . can be embedded in the hardware and software we deal with, in such a way as to make breach of contract [prohibitively] expens[ive] . . . for the breacher.”).

¹³⁴ Including, of course, the vending machine.

¹³⁵ See, e.g., Jaccard, *supra* note 11 (“[S]oftware, which computer code binds two, or a multitude, of parties in view of the execution of predefined effects, and that is stored on a distributed ledger.”).

operational control.¹³⁶ It bears emphasis, here, that there is an important difference between the two ways in which a system may be “distributed”: first, all elements of transaction verification and recording are (theoretically) open to anyone;¹³⁷ second, some elements of transaction verification and recording are open to a limited number of persons.¹³⁸ The models are described, respectively, as “permissionless” and “permissioned.”¹³⁹ Permissioned systems might usefully be illustrated by way of a Google Doc: a document can be set up so that a variety of persons may view or edit, while the infrastructure that allows the document to be created is maintained by a single company.

Unless the parties have the specific aim of setting up a transaction that ousts the operational control of either party (or any third party), there are considerable commercial advantages to a permissioned system. Take the following example:

Example 6: Two local authorities set up an interest-rate swaps agreement, which is intended to operate over a period of 20 years. They automate payments at designated intervals by way of interoperable scripts, with a user interface that allows them to see the state of their contract in real-time.

Let us suppose that in year three of the contract, the relevant government makes it illegal for local authorities to carry on agreements of this form. In these circumstances, it would be absolutely crucial for the parties to be able to halt performance. And there are, of course, many subtler alterations that organizations may wish to make in response to developments in their economic or legal environment. For these sorts of arrangements, negative automation is neither necessary nor desirable. And where negative automation is not the goal, a blind consensus protocol is not the right tool.

So, the second distinction is between positively-automated contracts (supported by permissioned protocols) and Szabo’s negatively-automated contracts (supported by blind consensus protocols). These two distinctions can be represented as four categories. The first two are types of code and can be

¹³⁶ Such a system may either use a centralized administering authority, or a smaller group of governing parties. *See, e.g.*, R3 & NORTON ROSE FULBRIGHT, CAN SMART CONTRACTS BE LEGALLY BINDING CONTRACTS?—AN R3 AND NORTON ROSE FULBRIGHT WHITE PAPER, https://lawsdocbox.com/Legal_Issues/72287181-Can-smart-contracts-be-legally-binding-contracts-an-r3-and-norton-rose-fulbright-white-paper.html (last visited Sept. 29, 2019).

¹³⁷ Like Bitcoin.

¹³⁸ R3’s “Corda” is such a model. *See* MIKE HEARN, CORDA: A DISTRIBUTED LEDGER (Nov. 29, 2016), https://docs.corda.net/_static/corda-technical-whitepaper.pdf.

¹³⁹ There may be a benefit to a variety of permissioned or permission-less models in adopting a chronological record of transactions; there will be a benefit to only *some* such models in grouping that record by mutually-referential blocks. *See generally id.*

called “plastic script”¹⁴⁰ and “persistent script.” Plastic script is (as the term is used here) any code that instructs a program to perform automatically, which remains in the control of one or more individuals. Persistent script is (as the term is used here) any code that instructs a program to perform automatically, which does not remain in the control of any individual(s). Plastic script is not given the label “smart contract”; persistent script is. The third and fourth categories are types of legal contract. All or part of a “positively-automated contract” is executed by a self-operating program; performance of a “negatively-automated contract” is prescribed by persistent script. Thus, there are four categories, three of which have attracted the label “smart contract”:

Figure 2:

Plastic script	Positively-automated contract
Persistent script	Negatively-automated contract

= smart contract

While I have divided these categories into distinct boxes, the reality is not so tidy. A contract might be “hybrid” in that parts of it may be negatively—and some parts positively—automated. Script may prescribe performance of a legal contract or some other arrangement. Moreover, there may be *degrees* of each form of automation; it may be made more or less difficult to interfere with performance, and a contract may require a limited form of ongoing input to execute.

So, if the “core case” of a smart contract describes the computer mechanism (persistent script) by which a contractual agreement is negatively automated, there exists a range of systems that admit greater or lesser degrees of operational interference. Our primary focus in Part III will be upon the merits of using persistent script to implement the sort of arrangement that Szabo envisaged—a negatively-automated legal contract.

¹⁴⁰ A type of script that may be shaped and altered by its creator, before and throughout contractual performance.

III. JUSTIFYING SMART CONTRACTS

We are now in a position to consider the benefits and disadvantages of using persistent script to perform contracts. The analysis in this part will revolve around three discrete but related claims that pervade the literature on smart contracting. Two claims are taxonomic. The first goes to the relationship between smart contracts and legal contracts, and it *denies* the distinction between code and contract that I drew at the end of Part II. The claim is that persistent script *is* a legal contract.¹⁴¹ The second goes to the relationship between smart contracts and the institutional law of contract. This claim is that, by ousting legal oversight,¹⁴² smart contracts stand in an “orthogonal” relationship to the law of contract.¹⁴³ The third, substantive, claim cuts to the heart of the normative question. The claim is that this competing transactional framework maximizes individual sovereignty.¹⁴⁴ I reject each claim in what follows.

A. *Smart Contracts and Legal Contracts*

Werbach and Cornell, whose analysis of smart contracts is one of the most nuanced and extensive, argue that persistent script (though just a “chunk of code”)¹⁴⁵ is nevertheless a legal contract.¹⁴⁶ For these authors, it is not

¹⁴¹ Werbach & Cornell, *supra* note 9, at 341–42 (The authors characterize smart contracts as a “chunk of code,” but conclude that “smart contracts are, at the conceptual level, still contracts. Though they might not constitute promises per se, smart contracts are voluntary mechanisms that purport to alter the rights and duties of the parties.”).

¹⁴² *Id.* at 339 (“*The central feature* of a smart contract—what supposedly makes them smart—is that legal enforcement will not be necessary, or even possible.” (emphasis added)).

¹⁴³ *Id.* at 363.

¹⁴⁴ The idea is that these features—code as contract, and smart contract as institutional competitor—combine to make consumers *better off*.

Ultimately, what makes smart contracts unique is that they grant contracting parties new tools to reduce monitoring costs and the potential for opportunistic behavior By decreasing the risk of opportunistic behavior, smart contracts open up new avenues for commercial relationships, potentially facilitating an increasing range of economic activities [S]mart contracts also provide comparable advantages when it comes to clarity, precision, and modularity.

THE RULE OF CODE, *supra* note 8, at 80–81.

¹⁴⁵ Werbach & Cornell, *supra* note 9, at 340–41 (“Do smart contracts involve promises or obligations? In a significant sense, ‘no.’ The smart contract sets in motion machinery that the parties cannot subsequently prevent. The smart contract is not fulfilled by some further action of a contracting party, but rather by the completion of this mechanical process.”).

¹⁴⁶ *Id.* at 341–42. In part because of the terminological difficulties to which I alluded above, opinions have been widely split on the question of whether a “smart contract” always, sometimes, or never constitutes a legal contract. Others take the view that only some such arrangements will constitute legal contracts. Green, *supra* note 11, at 234 (“There is no question, however, that a subset of those transactions *will* conform to the legal requirements of an enforceable contract”).

appropriate to draw the kind of distinction between persistent script and negatively-automated legal contract that I drew at the end of Part II. Instead, their table looks something like this:

Figure 3:

Plastic script	Positively-automated contract
Persistent script as negatively-automated contract

= smart contract

The argument behind their conclusion may be synthesized as follows. First, Werbach and Cornell define a contract as a “promise or an agreement that is legally enforceable.”¹⁴⁷ To the question of what *counts* as a legally-enforceable agreement, their answer is anything that is “meant to alter concretely the normative relation between the parties.”¹⁴⁸ This includes documents that “alter rights presently” such as a deed of conveyance.¹⁴⁹ Turning to the question of whether persistent script meets those requirements, they say:

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.¹⁵⁰

Thus, they conclude, “smart contracts are contracts.”¹⁵¹

¹⁴⁷ Werbach & Cornell, *supra* note 9, at 338.

¹⁴⁸ *Id.*

¹⁴⁹ *Id.* at 341 (“A deal may still count as a contract even though it leaves nothing open to be done or performed. A conveyance, for example, is a contract that alters rights presently, and does not involve any further, open promises.”).

¹⁵⁰ *Id.* at 342.

¹⁵¹

[S]mart contracts are contracts. They are agreements to shift legal rights and responsibilities, no less than an agreement between two parties physically exchanging goods for payment over a counter. Their status as contracts might be obscured by the fact that the parties intend litigation to be impossible, may

To focus analysis, let us summarize premises and conclusion as follows:

P1: A contract is a legally-enforceable agreement

P2: An agreement is intended to alter the parties' rights and duties

P3: A smart contract is intended to alter the parties' rights and duties

∴ A smart contract is a contract

I argue at the outset to this part that *P2* involves a crucial misstep. For the purposes of the law of contract, an agreement is intended to affect the parties' rights and duties in a *specific way*, which relates to the promised performance. I argue that persistent script, which does not encode these sorts of promissory obligations, is not a legal contract. Rather, by directing the performance of a contract, persistent script may have three kinds of impact on legal rights and duties. First, it may extinguish the promissory rights and duties of which the contract is constituted. Second, it may bring about a transfer of title, thereby altering the rights and duties entailed by ownership. Finally, it may trigger legal remedies where the conditions for contract formation are defective.

1. What Is a Contract?

Most definitions of “contract” focus on agreement.¹⁵² A contract is “an agreement giving rise to obligations which are enforced or recognized by law.”¹⁵³ Agreement is the factor “which distinguishes contractual from other legal obligations.”¹⁵⁴ Much of the definitional burden is thereby shifted: if a contract is an agreement that has a particular legal effect, what is an agreement?¹⁵⁵ The Oxford English Dictionary defines agreement as the act of coming to a “mutual

not make any promise, and may be expressed only in code. We suggest that these details do not alter the fact that smart contracts are, indeed, contracts . . .

See id. at 343.

¹⁵² *See, e.g.*, *Krasley v. Superior Court*, 161 Cal. Rptr. 629, 633 (Ct. App. 1980) (“The essence of a contract is the meeting of minds on the essential features of the agreement.”). Note that not all definitions share this emphasis. *See, e.g.*, RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 1981) (“A contract is a promise or a set of promises for the breach of which the law gives a remedy, or the performance of which the law in some way recognizes as a duty.”). Here, the emphasis is on the binding nature of a promise, which is intended to encompass the unilaterality of deeds.

¹⁵³ EDWIN PEEL, TREITEL ON THE LAW OF CONTRACT §1-001 (13th ed. 2011).

¹⁵⁴ *Id.*

¹⁵⁵ There are, of course, all sorts of agreements that never become promises, and all sorts of promises that occur without the law. The law exists at the fringes of consensual arrangements, to support a specific category of voluntary arrangement. Moreover, promises are not the central instance of voluntary obligations: two trusting parties will be content to operate wholly without exchanging promises. *See Joseph Raz, Promises and Morality in Law*, 95 HARV. L. REV. 916, 930–31 (1982) (reviewing P. S. ATIYAH, PROMISES, MORALS, AND LAW (1981)).

understanding,” or (understood as a legal term) “[a]n arrangement . . . made between two or more parties and agreed by mutual consent.”¹⁵⁶ Merriam-Webster defines agreement as “harmony of opinion, action, or character.”¹⁵⁷ Each such definition contains an emphasis upon mutuality: an “agreement” must have some sort of meeting of the minds. So, an agreement is something that occurs between two or more parties, and it involves an act of mutual consent.¹⁵⁸

There are, however, some further steps that we must make to understand the notion of a *contractual* agreement. There are two key differences between the way in which agreement is used outside of contract law (whether in the lay or legal sense) and the way in which agreement is used within contract law. First, the former may include statements about the past and present that carry no implication for the future: A and B may agree that “World War I began on July 28, 1914.” Or, to take a legal example, A and B might agree upon the location of their mutual property boundary. These are agreements, but they are not contracts.¹⁵⁹ Contractual agreements, by contrast, always refer to some *future* performance, yet to be rendered:

Example 7: A and B agree that A will write and deliver a manuscript about World War II by 5th July 2022; B will pay A \$1,000 in advance, \$1,000 on receipt of the completed manuscript.

In this example, each party promises to perform a particular act—A to write and deliver the manuscript, B to pay A \$1,000 now and \$1,000 upon timely delivery. So, a contract may involve an exchange of promises, or it may involve a conditional unilateral promise, but it always specifies some future performance.

Secondly, that agreement must be seriously meant. Werbach and Cornell put this as the claim that a contractual agreement includes anything that is “meant to alter concretely the normative relation between the parties.”¹⁶⁰ It bears emphasis, however, that the category of contractual agreement does not include

¹⁵⁶ *Agreement*, OXFORD ENG. DICTIONARY, <https://www.oed.com/view/Entry/4159?redirectedFrom=agreement#eid> (last visited Oct. 17, 2019). For this definition, the focus is upon the way in which parties interact.

¹⁵⁷ For this definition, the focus is upon the outcome of the parties’ interaction. *See Agreement*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/agreement?utm_campaign=sd&utm_medium=serp&utm_source=jsonld (last visited Sept. 29, 2019).

¹⁵⁸ *See* MARGARET JANE RADIN, *BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW* 66 (2014) (“What is the difference between agreement and the notions of consent or assent? Agreement seems to imply more of a two-sided process (the idea of two parties coming to an agreement, the idea of discussion or negotiation, what contracts scholars tend to call ‘dickered terms’). Consent seems to imply instead a one-sided process . . .”).

¹⁵⁹ Of course, the promise to forbear from suing in respect to some dispute concerning property boundary could constitute contractual consideration.

¹⁶⁰ Werbach & Cornell, *supra* note 9, at 340.

any set of legal relations, or any set of (bilateral or multilateral) rights and duties. Take the following example:

Example 8: A female employee (“E”) of a firm (“F”) decides not to wear high-heeled shoes, in contravention of F’s code of conduct. E does so with the intention of inciting F to terminate her contract, so that she can draw media attention to gender inequalities in F’s code of conduct. E goes to work wearing flat shoes, and F does in fact terminate E’s contract.

In this example, E performs an act that is intended to “alter concretely the normative relation” between herself and F; she intends to incite F to sack her. Clearly, however, E’s act is not a contract. Contracts alter legal relations in a *specific way*. The normative impact of a contractual agreement is the imposition of a legal obligation in respect of the promised performance—in Example 7, to write and deliver a manuscript, and to pay the agreed price.

Of course, performing the contract may affect the parties’ legal positions in other ways. Performing the contract correctly will extinguish the rights and duties that relate to performance. That performance may also involve the transfer of a particular right, such as title to a book or (to use Werbach and Cornell’s example of a conveyance) the transfer of title to a house. Performing incorrectly, or not at all, may give rise to secondary rights and duties in respect of breach. And if there is some defect in the intention of the contracting parties, the parties may acquire the secondary, remedial right to unwind the transaction.

So, a contract is an agreement between two or more parties in respect of some future performance, which gives rise to corresponding bilateral rights and duties in respect of that performance. The *execution* of a contract entails various derivative and distinct normative effects. These effects always include extinguishing the right to performance (and the corresponding duty) and may include the transfer of title or secondary, remedial rights and duties.¹⁶¹

2. Code and Contracts

Let us turn now to the contractual status of ordinary scripting code. According to Savelyev, there is a fundamental similarity between the linguistic structure of code, and that of contract: “computer code is based on statements like “if ‘x’ then ‘y.’” “Such an approach is in harmony with contractual terms and conditions.”¹⁶² This might encourage the conclusion that there is nothing

¹⁶¹ The former may exist without the latter, and vice versa. It is possible to have an agreement that does not involve the change in ownership of any asset. Or one may hypothesize an agreement in which one party agrees to mow the other’s lawn, in return for which the other will collect his children from school 3 days a week. It is possible to have a change in ownership of an asset without an exchange of promises: a gift is of this kind.

¹⁶² Savelyev, *supra* note 11, at 126; see also Lord Hodge, Justice, Supreme Court of the U.K., Financial Technology: Opportunities and Challenges to Law and Regulation at East China

substantive that distinguishes code from the written text that might contain the terms of a contractual agreement.¹⁶³ There is, however, an important difference between two kinds of conditions, which affects the conclusions that we may draw about the constitute role of code.

The first type of condition is normative, and it is the one regularly formalized by way of contract terms. Let us return to Example 1.1:

Example 1.1: S owns and runs a convenience store. Soda is advertised for sale at a price of \$1/can. B selects a can, hands \$1 to S at the counter, and exits the store with the drink.

This relationship is normatively conditional: if x (payment of money) then S promises to do y (transfer of soda). And because S promises to do y , we can say that S *ought* to do y . B and S have formed an agreement involving an exchange of promises that relate to performance.

The second type of condition is purely causal.¹⁶⁴ Contrast Example 1.1 with Example 1.3:

Example 1.3: S owns and stocks a vending machine, in which soda is offered for sale at a price of \$1/can. B selects a can, puts coins of the correct value in the slot, and recovers the drink from a tray at the base.

Here, the connection between payment (input) and delivery (output) is conditional: if x then y . But it is *not* normative. The vending machine is arational. It cannot enter into agreements or respond to reasons. A vending machine simply *executes* the terms of a contractual agreement between S and B. That contract, we have seen, adopts the form of an open, unilateral offer, which is accepted when B puts the coins into the slot.¹⁶⁵ That transaction has the same sort of normative impact as the conveyance. It transfers title to the drink to B, thereby extinguishing the promissory obligation owed by S.

University of Political Science & Law, Shanghai, China, 14 (Oct. 26, 2018), <https://www.supremecourt.uk/docs/speech-181026.pdf>.

¹⁶³ See, e.g., Werbach & Cornell, *supra* note 9, at 342 (“Nothing, so far as we can tell, prevents an expression of mutual assent from being formulated in code.”); see also Surden, *supra* note 82, at 656 (“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.”). For a study of the habitual confusion of the legal document and the instrument it encodes, see Mark Greenberg, *The Moral Impact Theory of Law*, 123 YALE L.J. 1288, 1309 (2013); Mark Greenberg, *Legislation as Communication? Legal Interpretation and the Study of Linguistic Communication*, in PHILOSOPHICAL FOUNDATIONS OF LANGUAGE IN THE LAW 217 (Andrei Marmor & Scott Soames eds., 2011); Frederick Wilmot-Smith, *Term Limits: What Is a Term?*, OXFORD J. LEGAL STUD. (forthcoming).

¹⁶⁴ To be distinguished from an implicational relationship.

¹⁶⁵ *Supra* Section II.A.2.

This distinction is crucial to understanding the way in which computers typically interact with legal norms. When we express contractual terms in writing, we thereby “encode” the obligations created by an exchange of promises. The contract specifies the parties’ rights and duties in relation to the promised performance (“promissory duties”). Creation of the contract triggers the moral and legal “ought”: S and B ought to do as their contract says. When we translate those obligations into scripting code, we do so in the form of instructions to a computer.¹⁶⁶ We might say that the computer is “obliged to” or “must” perform, so long as we are clear about what this means: the computer cannot do otherwise than perform, given certain stipulations. If we say that the computer “ought” to perform, we are no longer specifying a normative duty, but simply a probabilistic prediction. While S and B are under a (moral and legal) duty to perform, the computer simply *has* to perform.¹⁶⁷

This is not to deny that it is literally possible to write “S is obliged to do x” in code.¹⁶⁸ Or otherwise, that if two computer-literate parties exchanged copies of code until they reached a consensus as to the intended output, they could thereby generate obligations to bring about the performance that the code prescribes—without the need for an independent expression of their intent.¹⁶⁹ It is simply to be clear about the difference between specifying promissory duties in the process of constituting a contract and discharging promissory duties in the process of executing a contract.¹⁷⁰

¹⁶⁶ See Surden, *supra* note 82, at 658 (“The basic idea behind a computable contract term is to create a series of actionable, computer-processable instructions that approximate what it is that the parties are intending to do in their contractual arrangement.”).

¹⁶⁷ Of course, we literally could add the term “obliged to” into code that is designed to execute the contract, but it would be adding nothing to what we have already produced by setting up the contract.

¹⁶⁸ One Twitter user (Jason Morris @RoundTableLaw) kindly provided me with the following example: “Obliged(A,ProvideGumballTo(B)) :- HasGumballs(A),InsertsQuarterInto(B,A).” With this, it is apparently possible to ask “to whom is Jason obliged to provide gumballs?” Obliged (Jason,ProvideGumballTo(?X)), and get a useful answer. Jason Morris (@RoundTableLaw), TWITTER (Dec. 13, 2018, 3:20 AM), <https://twitter.com/RoundTableLaw/status/1073175822737887232>).

¹⁶⁹ Given certain conditions, there may be advantages to generating rights and duties in this way, though Surden describes in detail the types of obstacles that arise from the distinction between “natural language” and computer code, some of which may be resolved by the use of devices such as “threshold agreements” or “data standards.” See Surden, *supra* note 82, at 651–52.

¹⁷⁰ Werbach and Cornell appear to draw something like this distinction:

As an analogy, if Bob balances a pail of water on top of a door, he does not promise to drop water on whoever next opens the door. Rather, he has merely set up the mechanical process by which that will inevitably happen. In a similar way, a smart contract to transfer one Bitcoin upon such-and-such event occurring is not really a promise at all. A smart contract would not say, “I will pay you one Bitcoin if such-and-such happens,” but rather something like, “you will be paid one Bitcoin if such-and-such happens.”

Werbach & Cornell, *supra* note 9, at 340.

With this in mind, let us return to Example 2.2:

Example 2.2: an online newspaper accepts payment in Bitcoin. If a reader (“B”) pays ₿0.01, B is automatically granted a one-month subscription.

In this example, the code prescribes rules according to which a computer is to perform a particular action, in discharge of a promissory duty generated by B’s payment. The script is not itself a contract; it executes a contract.

Putting script on a blind consensus platform does not change the nature of the normative interaction. Let us return to Example 3.1:

Example 3.1: S offers a cryptokitty (“Kitty 572634”) for sale for ₿1. S also uploads script that, when triggered by payment, will cause the cryptokitty to be transferred to the buyer. B transfers ₿1 and receives Kitty 572634.

The essence of a contract is to create rights and duties with respect to performance. Persistent script does not encode (though it may execute) promissory obligations. It is not, therefore, a contract. As above, the code executes the underlying contract.¹⁷¹

3. Code and Ownership

In Example 3.1, executing the code discharges S’s promissory duty to transfer the cryptokitty.¹⁷² Indeed, it does so without permitting S to derogate from contractual performance. Thus, it precludes any secondary, remedial rights and duties that might otherwise arise from non-performance. Executing the code may also affect the rights and duties entailed by legal ownership: Where once Kitty 572634 belonged to S, now it belongs to B; where once one unit of Ether belonged to B, now that unit belongs to S. But that title-transfer is not *itself* a contract. The change in legal relations entailed by the transfer of ownership is part of the normative fallout of contractual performance.

We are now in a better position to understand the claim that “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*.”¹⁷³ The code that effects a transfer of ownership from one party to another does not constitute the contract between transferor and transferee; it executes that contract. There remains an important distinction between the exchange of promises and the instantiating code.

¹⁷¹ See also MICHÈLE FINCK, BLOCKCHAIN REGULATION AND GOVERNANCE IN EUROPE 25 (2019) (“A smart contract is, essentially, a sequence of instructions that a miner runs in exchange for compensation.”).

¹⁷² Finck, *supra* note 11.

¹⁷³ Werbach & Cornell, *supra* note 9, at 342 (emphasis added).

Yet, the question of ownership is less straightforward than that claim might belie. Whether the transaction does indeed affect the rights and duties entailed by ownership depends upon whether, at the outset, the parties actually “own” those assets in law. We might usefully distinguish, here, between two kinds of digital asset. The first is an asset that *represents* some other real-world asset. The second is an asset that only exists in a virtual environment.

For present purposes, a “symbolic asset” is an asset that represents another real-world asset, and a “symbolic crypto-asset” is an asset that represents another real-world asset, and which exists on a blind consensus platform. Take the following example:

Example 9: S offers a car for sale for ₦5. B transfers ₦5 to S’s wallet, thus triggering a program that grants access to the car via e-key to B.

In such a case, the question of whether entitlement to the car has been transferred is a legal question. The legal system is involved to determine (at minimum) whether the transaction transfers ownership and to regulate cases of title-conflict.

One might argue that these questions can be settled in an extra-legal way. Perhaps the law does not recognize the transfer as a valid car-sale. *Nevertheless*, both parties are happy to treat it as if it were. This is conceptually possible, but there are good reasons to think it impracticable. Unless S wishes to be saddled with tax and insurance for the following year, S will want to ensure that B is the registered keeper. If someone interferes with the car, B will want to be at the helm of any legal suit. For so long as the legal system produces different answers from the transactional matrix of a blind consensus protocol, these sorts of issues will arise.¹⁷⁴

For present purposes, a “pure asset” is an asset that exists only in the digital sphere. And a “pure crypto-asset” is an asset that exists only on a blind consensus platform, or which has some other virtual manifestation. Bitcoin falls into this category; so do cryptokitties.¹⁷⁵

Example 3.1: S offers a cryptokitty (“Kitty 572634”) for sale for ₦1. S also uploads script that, when triggered by payment, will cause the cryptokitty to be transferred to the buyer. B transfers ₦1 and receives Kitty 572634.

In our Example 3.1, the question of legal ownership is not straightforward. Assuming that we can discharge the burden of identifying the appropriate

¹⁷⁴ See Edmund Schuster, Assoc. Professor of Law, London Sch. of Econ., Proceedings of LSE Law Seminar “Cryptoassets and the Law”: The Empty Promise of Cryptoassets and Smart Contracts (Sept. 4, 2018), <https://personal.lse.ac.uk/schustee/crypto.html>.

¹⁷⁵ And the digital land-holding platform known as “Decentraland.” See DECENTRALAND, <https://decentraland.org/> (last visited Sept. 29, 2019).

jurisdiction,¹⁷⁶ each such jurisdiction may offer a different answer to the question of whether a person may legally “own” a digital asset.¹⁷⁷ If the relevant legal system does not formally recognize the legal status of holding, it follows that the transfer does not have an impact on the legal entitlement of the parties. If S and B did not own Kitty 572634 and $\Xi 1$ respectively before the exchange, they will not own $\Xi 1$ and Kitty 572634 afterwards.

However, it is worth emphasizing that the law does not exhaust the possible normative effects of digital asset transfers. One of the best examples of this is a case known as the “DAO heist,”¹⁷⁸ upon which our Example 4 was modelled:

Example 4: A set of interoperable scripts control digital wallets to which platform users may commit funds during a designated window. Those scripts are designed to direct a series of investments over a fixed period of time, paying any investment return to users in proportion to funds committed.

At the beginning of May 2016, members of the Ethereum community announced the launch of the Decentralized Autonomous Organization (known as “the DAO”), an application that was intended to operate like a venture capital fund. During a specified period, anyone could send Ether to a special wallet address in exchange for DAO tokens. The launch outstripped expectations, attracting $\Xi 12.7\text{m}$ (then worth around \$150m). On June 18, 2016, members noticed that funds were disappearing from the DAO, and it transpired that a hacker had initiated a series of transactions, known as a “recursive call exploit,” in which the DAO paid Ether multiple times before the program could update its own balance.

Following the hack, members were faced with a choice: either they could accept its consequences or revise the transaction history (creating a “hard fork”)

¹⁷⁶ See generally FIN. MKTS. LAW COMM., DISTRIBUTED LEDGER TECHNOLOGY AND GOVERNING LAW: ISSUES OF LEGAL UNCERTAINTY (March 2018), http://fmcl.org/wp-content/uploads/2018/05/dlt_paper.pdf.

¹⁷⁷ The U.S. and the UK offer different approaches. In the UK, the conclusion has been firm: digital assets cannot be owned. See, e.g., *OBG v. Allan* [2008] 1 AC 1 (appeal taken from Eng.); *Your Response Ltd. v. Datateam Business Media Ltd.* [2014] EWCA Civ 281 (appeal taken from Eng.). For a workaround for unique assets, see *Armstrong v. Winnington* [2012] EWHC 10 (Appeal taken from Eng.). In the U.S., unique digital assets such as domain names can be the object of claims to protect property. See *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003) (“Registering a domain name is like staking a claim to a plot of land at the title office. It informs others that the domain name is the registrant’s and no one else’s.”).

¹⁷⁸ See Michael del Castillo, *The DAO Hacker Is Getting Away*, COINDESK (Aug. 10, 2016), <https://www.coindesk.com/ethereum-dao-hacker-getting-away-classic>; Samuel Falkon, *The Story of the DAO—Its History and Consequences*, MEDIUM (Dec. 24, 2017), <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>; Klint Finley, *A \$50 Million Hack Just Showed that the DAO Was All Too Human*, WIRED (June 18, 2016, 4:38 AM), <https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>.

that would allow participants to recover Ether from the DAO. That question was a normative one: who *ought* to be entitled to the Ether captured by the heist? Those who opposed the hard fork argued that the hack had occurred within the rules of the DAO and should be left alone. This type of claim has come to be known as “immutability,” and its thrust is that the code governs every aspect of the transactional infrastructure; there is no room for additional “soft” values.¹⁷⁹ Those who supported the hard fork argued that there was something ethically impermissible about the hacker’s actions, which the community’s response ought to reflect. Ultimately, a majority of miners were convinced to implement the fork. For those running the new software, the DAO hack had never happened, and the participants recovered their funds.¹⁸⁰

Thus, the rules that govern the transfer of digital assets express normative commitments. Those commitments may be external (legal) or internal (otherwise an expression of the social consensus of a particular group), but they cannot be avoided.

4. Language Games

Wittgenstein famously argued that there is no reason to look for one essential “core” of a word’s meaning that is common to all uses of that word.¹⁸¹ Instead, he claimed, we should acknowledge a “complicated network of similarities overlapping and criss-crossing,”¹⁸² admitting into these categorical definitions examples that bear only “family resemblances” to one another.¹⁸³ It would appear that lawyers and programmers are content to use “smart contract” in this sort of way—confident that there is some sufficiently-overlapping meaning in the different uses of the term to elucidate broader questions about utility, efficiency, risks, etc. There are reasons to think this confidence misplaced. In particular, two types of missteps have emerged from the confluence of fields.

First, the ideas of positive and negative automation have become muddled. Lawyers laud the advantages of contractual automation but suggest

¹⁷⁹ See WERBACH, *supra* note 17, at 492–94; Werbach & Cornell, *supra* note 9, at 327.

¹⁸⁰ See Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (July 20, 2016), <https://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds>.

¹⁸¹ See generally LUDWIG WITTGENSTEIN, *PHILOSOPHICAL INVESTIGATIONS* (1953).

¹⁸² *Id.* at 66.

¹⁸³ *Id.* For instance, we feel wholly comfortable discussing the concept of a “game,” without ever requiring consensus upon identifiable pre-requisites: “game” might describe a two-player game, but also includes solitaire; “game” might describe a game of skill, or one of chance.

that blockchain technology is required to underpin this sort of smart contract.¹⁸⁴ This conceptual chimera is a positively-automated smart contract underpinned by a blind consensus protocol. I sought to show in Part II of this article that persistent script is *not* necessary to facilitate positive automation. Permissioned ledgers support positively-automated contracts.

The second problem has been the focus of Part III so far. The idea that smart contracts oust legal oversight has led to the conclusion that programs are able to carry the bulk of the normative weight: programs *are* contracts, operating in tandem with traditional promissory relationships.¹⁸⁵ The purpose of this section has been to show that persistent script is not itself a contract, though it may execute a contract. And in so doing, it may have a number of other (legal or alegal) normative effects.

At this juncture, we may return to Figure 2:

Plastic script	Positively automated contract
Persistent script	Negatively-automated contract

= smart contract

“Smart contract” may refer to persistent script, or it may refer to a legal contract that is implemented through persistent or plastic script. It cannot at once refer to both. Contracts and code interact in complex and nuanced ways, but there *are* reasons to maintain, rigorously, the conceptual boundaries between them.

B. Smart Contracts and the Law of Contract

We are now in a position to turn to the relationship between persistent script and the institutional law of contract. Here, Werbach and Cornell make their second taxonomic claim. They argue that smart contracting does not interact

¹⁸⁴ See, e.g., Green, *supra* note 11, at 234–35 (“Smart ‘contracts’ are self-executing agreements that exist as a set of instructions to a computer This has been made possible by the advent of distributed ledger technology.”).

Fundamentally, a “smart contract” is a set of coded computer functions . . . [which] allows self-executing computer code to take actions at specified times and/or based on reference to the occurrence or non-occurrence of an action or event The smart contract is stored and operates on Blockchain.

See *A Primer on Smart Contracts*, *supra* note 28.

¹⁸⁵ See, e.g., Werbach & Cornell, *supra* note 9, at 343.

directly with, but rather stands in an “orthogonal” relationship to, contract law.¹⁸⁶ For Werbach and Cornell, smart contracts are contracts that exist outside the boundaries of the law.

In what follows, I challenge both the remedial view of contract law and the claim that smart contracts completely oust legal oversight. I argue that smart contracting adversely affects the ability of contract law to support valuable relationships of trust and reliance.

1. What Is Contract Law?

Werbach and Cornell argue that contract law exists primarily “to adjudicate the justice of a situation *ex post*,”¹⁸⁷ rather than to “alter our reasons going forward.”¹⁸⁸ This, they say, lies at the heart of the distinction between “smart contracts” (understood as a type of non-executory contract) and the law of contract (understood as a set of institutional responses to promises). Werbach and Cornell begin their discussion by imagining the following scenario: Abby promises Bob that she will pay back Bob’s loan to her.¹⁸⁹ By promising, they say, “Abby creates a moral obligation. She now has a special sort of reason to pay the money back.”¹⁹⁰ They continue: “Contract law does not change anything about Abby’s obligations. Those were complete the moment that she promised.”¹⁹¹ Instead, contract law “enables an avenue for Bob to complain if Abby does not fulfil her obligations.”¹⁹² The law of contract is, in short, a remedial institution.¹⁹³ The impact of smart contracts, they say, is to “eliminate the act of remediation by admitting no possibility of breach.”¹⁹⁴ Thus, they conclude: “[I]t is apparent that smart contracting does not even purport to do what contract law does. The two have fundamentally different objectives. Smart contracting functions to ensure action. Contract law functions to recognize and remedy grievances.”¹⁹⁵ For Werbach and Cornell, smart contracts are legal contracts that (somewhat paradoxically) exist outside of the law of contract.¹⁹⁶

¹⁸⁶ *Id.* at 363.

¹⁸⁷ *Id.* at 361.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.* at 362.

¹⁹⁰ *Id.*

¹⁹¹ *Id.*

¹⁹² *Id.* at 362–63.

¹⁹³ *Id.* at 361 (“[C]ontract law is a fundamentally remedial institution, not aimed at creating new reasons to perform, but aimed at resolving disputes, taking those reasons as already given.”).

¹⁹⁴ *Id.* at 318.

¹⁹⁵ *Id.* at 363.

¹⁹⁶ *Id.* (“[S]mart contracting does not even purport to do what contract law does. The two have fundamentally different objectives. Smart contracting functions to ensure action.”).

This, I think, raises an important point about the way in which we conduct the taxonomic exercise. We might categorize according to the “formal structure”¹⁹⁷ of a claim. For instance, “[a] wrong is a breach of a duty owed to someone else The law of torts is concerned with the secondary obligations generated by the infringement of primary rights.”¹⁹⁸ According to this sort of categorization, the law of torts and contract belong together;¹⁹⁹ both are part of the corrective enterprise entailed by undoing breaches of duties, whatever the justificatory basis of that enterprise.

This clearly is not what Werbach and Cornell have in mind. For those authors, it is important that the law of contract responds to breaches of specific *types* of obligation, which are those generated by a promise.²⁰⁰ So, they care not just about the formal pattern of the law, but also about the *source* of the legal obligation. But this begs a further question: Why does it matter that the obligation to which the law of contract responds is promissory? What makes promises special?

It is widely accepted that those who practice the law must “treat like cases alike.”²⁰¹ At its most basic, this demands that we have some sense of what counts in favor of a particular treatment: on what basis are we to say that it is relevant that a case involves a promise, but that it is *not* relevant that the promise was made on a Monday, rather than a Tuesday (or any other day of the week)? That distinction is a normative one. The similarities and differences between two cases are discerned by reference to the reasons why a particular legal response *ought* to follow.²⁰²

¹⁹⁷ Frederick Wilmot-Smith, *Reasons? For Restitution?*, 79 MOD. L. REV. 1116, 1118 (2016).

¹⁹⁸ ROBERT STEVENS, TORTS AND RIGHTS 2 (2007).

¹⁹⁹

The norms in this second set can be unified even if they are justified by quite different reasons or protect different interests. On Stevens’ model of torts, for example, the norms are unified regardless of the reasons for the primary rights: contractual rights arise due to voluntary undertakings; rights to physical integrity arise regardless of voluntary undertakings.

See Wilmot-Smith, *supra* note 197, at 1118.

²⁰⁰ Werbach & Cornell, *supra* note 9, at 361–63.

²⁰¹ See, e.g., H.L.A. HART, THE CONCEPT OF LAW 155 (1961); ANDREI MARMOR, LAW IN THE AGE OF PLURALISM 183–97 (2007).

²⁰² Webb argues,

Cases which differ in various respects are nonetheless alike if their shared features, however few, are sufficient to require their like treatment [W]e can determine whether cases really are alike only by inquiring into what reasons bear on their proper treatment. Their likeness is then a function of the reasons that apply alike to them

CHARLIE WEBB, REASONS AND RESTITUTION 44–45 (2016).

Different types of justification are offered for the rights and duties that contract law supports, and the way in which it supports them.²⁰³ For some, contract law meets demands of individual autonomy; it responds to the desire to create the greatest possible range of free will.²⁰⁴ For others, the law of contract seeks to maximize welfare (where “welfare” can mean wealth, happiness or some other aspect of wellbeing).²⁰⁵ But all such explanations share a common emphasis: whatever is the precise justificatory basis for the law of contract, it concerns the *voluntariness* of the parties’ arrangement.²⁰⁶ Contracts embed (support or constitute) voluntary obligations.²⁰⁷

Thus, the claim that the law of contract is “remedial” does not excuse us from enquiring into the justification for a particular remedial response that belongs to the category of contract law. Whichever form it takes, that justification relates to the choices through which individuals shape their own affairs. With this in mind, let us turn to the relationship between smart contracting and the law of contract.

2. Smart Contracting and Contract Law

We saw above that the second step of Werbach and Cornell’s analysis is whether that smart contracts *preclude* legal remedial oversight. Smart contracts “eliminate the act of remediation,” they say, “by admitting no possibility of breach.”²⁰⁸ There is one sense in which this is clearly true. We have seen that the unique feature of persistent script is that (once uploaded) the code cannot be altered and (once triggered) it cannot be prevented from executing. I have called this “negative automation.” To the extent that persistent script performs a legal contract, it precludes the remedial obligations that might otherwise arise from mis-performance.²⁰⁹

²⁰³ For a summary, see RADIN, *supra* note 158; STEPHEN A. SMITH, CONTRACT THEORY Part II (2004); MICHEAL J. TREBILCOCK, THE LIMITS OF FREEDOM OF CONTRACT (1997).

²⁰⁴ See, e.g., CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION (1981); Peter Benson, *The Unity of Contract Law*, in THE THEORY OF CONTRACT LAW: NEW ESSAYS 118 (Peter Benson ed., 2001).

²⁰⁵ For the view that this utility is wealth, see generally RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (1973).

²⁰⁶ See generally FRIED, *supra* note 204; P.S. ATIYAH, PROMISES MORALS, AND LAW (1981); T.M. SCANLON, WHAT WE OWE TO EACH OTHER (1998); Richard Craswell, *Contract Law, Default Rules, and the Philosophy of Promising*, 88 MICH. L. REV. 489 (1989); Charles J. Goetz & Robert E. Scott, *Enforcing Promises: An Examination of the Basis of Contract*, 89 YALE L.J. 1261 (1980); Daniel Markovits, *Contract and Collaboration*, 113 YALE L.J. 1417 (2004); Alan Schwartz & Robert E. Scott, *Contract Theory and the Limits of Contract Law*, 113 YALE L.J. 541 (2003).

²⁰⁷ Joseph Raz, *Promises and Morality in Law*, 95 HARV. L. REV. 916, 933 (1982).

²⁰⁸ Werbach & Cornell, *supra* note 9, at 318.

²⁰⁹ Or non-performance.

But there are other things that may go wrong with a contract. There may, for instance, be problems with contract *formation*. Where a contract is entered into by mistake, on the basis of some fraudulent misrepresentation or other unconscionable conduct, it may be open to the party affected to unwind the transaction. This sort of remedy is known as rescission,²¹⁰ and the task of restoring the parties to the financial position in which they were prior to the transaction is called “restitution.”²¹¹ We can exemplify rescission and restitution by returning to Example 7:

Example 7: A and B agree that A will write and deliver a manuscript about World War II by July 5, 2022; B will pay A \$1000 in advance, \$1000 on receipt of the completed manuscript.

Let us imagine that A has represented to B that A is a law professor, and B makes the contract on this basis. In fact, A is a first-year student in linguistics. And let us suppose that B discovers the truth after paying the \$1000 advance. At this point, A may choose to rescind (unwind) the contract and seek restitution (return) of the \$1000.

It is often said that transactions that occur within the context of a blind consensus protocol are “irrevocable.”²¹² But the inability of one or both of the parties to undo the transaction *in specie* does not preclude restitution.²¹³ In fact, this happens often: a payment instruction is irrevocable once acted upon by participating banks, but a payor may nevertheless obtain a money award that restores payor and payee to their pre-payment position. In principle, that remedy is accessible to those who use smart contracts. The aggrieved party in each of the following examples (each of which has occurred in practice in many different forms) could, in principle, sue for restitution:

Example 3.2: S offers a cryptokitty (“Kitty 572634”) for sale for £1. B accidentally transfers £10 to S’s wallet, which triggers a program that transfers Kitty 572634 to B.

Example 3.3: S offers a cryptokitty (“Kitty 572634”) for sale for £1. B transfers £1 to S’s wallet, which triggers a program that—

²¹⁰ See generally DOMINIC O’SULLIVAN ET AL., *THE LAW OF RESCISSION* (2012).

²¹¹ *Id.*; see also CHARLES MITCHELL ET AL., *GOFF & JONES: THE LAW OF UNJUST ENRICHMENT* (2016).

²¹² Werbach & Cornell, *supra* note 9, at 335 (“Even though blockchain transactions are irrevocable, there are ways to build in more flexibility. There is no technical means, short of undermining the integrity of the entire system, to unwind a transfer. It is, however, possible to incorporate logic into a smart contract that permits exceptions or conditions.”).

²¹³ We already offer these avenues of recourse for ordinary financial transactions: once acted upon by participating banks, payment instructions are technically irrevocable; nevertheless, parties can either sue their counterparty directly, or obtain the help of their banks, in order to recover the financial equivalent of reversing the transaction *in specie*.

because of a flaw in its code—transfers Kitty 572634, Kitty 572635, and Kitty 572636 to B.

Example 3.4: S offers a new type of crypto-coin, a “KittyCoin,” for sale at a price of $\text{€}0.1$, promising that each coin will rise in value ten-fold once S’s new digital cat-grooming parlour is launched. B buys 100 KittyCoins. S has no intention of launching a digital cat-grooming parlour, and the KittyCoins become worthless.

While it is not possible to alter the code itself, it is possible to correct the imbalance created by the defect in formation or performance. In Example 3.2, S could be required to pay B $\text{€}9$ or its money-equivalent. In Example 3.3, B could be required to retransfer Kitty 572635 and Kitty 572636 or pay S their monetary value. And in Example 3.4, S could be required to restore $\text{€}10$ or its monetary equivalent to B. But here, it is important to note that the use of persistent script raises practical questions concerning how easy it is for parties to access the law’s remedial infrastructure.

Three types of obstacles may arise. The first and simplest goes to the lack of operational control over persistent script. Even if the mistake in Example 3.3 is known to S prior to contractual performance, S’s only recourse is to sue after the fact. This is the function of negative-automation: no one can interfere with performance. And this is where parties may face their second problem, which concerns the ability to *identify* one’s counterparty. Bitcoin and Ethereum permit users to transact pseudonymously so that few actually know the real-world identity of the counterparty. That identity is almost always practically impossible to ascertain.²¹⁴ And the inability to identify one’s counterparty is, of course, an insuperable obstacle to any putative legal claim.²¹⁵

The third obstacle, which I address in detail in the final section of this article, concerns *disintermediation*. Traditional intermediaries often play a key role in both preventing and solving problems with contract formation. Consumers must take cautionary steps before executing payments, and banks will unwind payments obtained through fraud or by mistake. Retail platforms such as Amazon and eBay offer a broad and flexible remedial infrastructure, providing effective insurance against contractual performance that mismatches the consumer’s expectations.

²¹⁴ There are also heuristics through which sophisticated actors can narrow-down candidates, but these tools are altogether inaccessible to consumers. *See generally* SARAH MEIKLEJOHN ET AL., A FISTFUL OF BITCOINS: CHARACTERIZING PAYMENTS AMONG MEN WITH NO NAMES (2013), <http://discovery.ucl.ac.uk/1490261/1/Meiklejohn%20et%20al%20A%20fistful%20of%20bitcoin%20s.pdf>.

²¹⁵ THE RULE OF CODE, *supra* note 8, at 85 (“The autonomous nature of smart contracts also creates complications in commercial arrangements involving pseudonymous parties To file a lawsuit, an injured party will need to know the identity of the opposing party.”). Of course, if participants might be willing to retransfer the money, but you are beholden to the character of your (unidentified) counterparty.

In the absence of intermediaries, and in light of the difficulties of counterparty identification, the risks associated with contractual defects (in formation of the contract, or in the underlying code that executes it) must be absorbed by the consumer.²¹⁶ In the final Section of this paper, I consider how this affects the overarching assessment of the merits of smart contracting; here, our focus is upon how that practice relates to the law of contract.

In one sense, the goals of smart contracting and the law of contract align. Persistent script offers an effective alternative mechanism for enforcing promissory obligations. To the extent that negative automation limits the potential for operational interference, contracting parties may be surer of achieving their intended goal.²¹⁷ Understood instrumentally, there is a natural affinity between contract law and unbreakable contracts. Yet, there are also important ways in which smart contracting frustrates the goals of contract law, which go to the quality of the parties' relationship.

The first concerns the nature of any ordinary contractual relationship that may be generated by smart contracts. If the claim is that contract law is justified when it supports valuable relationships of trust and confidence,²¹⁸ eliminating the need for trust in one's counterparty *erodes* the qualities that make those relationships valuable.²¹⁹ We may distinguish here between "thick" and "thin" trust. Thick trust exists in the context of a trusting relationship; parties have a general confidence that their counterparty's intentions conform to their outward manifestation.²²⁰ Thin trust is mere confidence in counter performance.²²¹ By securing the latter, smart contracting obviates the former.

The second concerns the quality of a contractual relationship induced by (negligent or fraudulent) misrepresentation, improper pressure, or some other

²¹⁶ See Werbach & Cornell, *supra* note 9, 346–47 ("With a smart contract, there is no one to restrain, because the smart contract code is immutable once embedded in the blockchain. A smart contract could even include terms that are illegal, unconscionable, or otherwise legally unenforceable.").

²¹⁷ See *id.* at 360 ("[B]ecause the agreed-upon result occurs automatically, uncertainty about performance, and about judicial recognition, disappears. A promisee no longer needs to wonder whether the promise will be kept, or whether a court will recognize the breach.").

²¹⁸ What Saprai calls "trust-based cooperation." PRINCE SAPRAI, *CONTRACT LAW WITHOUT FOUNDATIONS: TOWARDS A REPUBLICAN THEORY OF CONTRACT* (forthcoming 2019). Raz argues that promises create a "special bond" between promisor and promisee. Joseph Raz, *Promises and Obligations*, in *LAW, MORALITY, AND SOCIETY: ESSAYS IN HONOUR OF H. L. A. HART* 210, 227–28 (P.M.S. Hacker & Joseph Raz eds., 1977). Markovits prefers a theory of contract as an institutional response to the need to "sustain collaborative agreements among individual persons." Markovits, *supra* note 206, at 1472.

²¹⁹ On the process of that erosion in relation to boilerplate contracts, see RADIN, *supra* note 158.

²²⁰ So that their counterparty will in fact exclude (most) reasons against performance.

²²¹ Though he does not put it thus, see DORI KIMEL, *FROM PROMISE TO CONTRACT: TOWARDS A LIBERAL THEORY OF CONTRACT* (2005).

unconscionable conduct.²²² We saw above that all theories of contract relate in some way to the underpinning consent of the contracting parties.²²³ Thus, the law of contract not only encourages parties to abide by their promises; it also contains a range of mechanisms for allowing the parties to escape from ill-formed contracts and oppressive terms. To the extent that smart contracting makes it harder for parties to escape transactions that do not embody any of the (intrinsic or instrumental) relational virtues that the law of contract upholds, that practice comes into direct conflict with the goals of contract law.

Thus, the practice of smart contracting *does* interact with the law of contract, and there are reasons to think that that interaction will not always be a harmonious one. Here, we arrive at the broader question that lies at the heart of this analysis: do smart contracts enhance individual sovereignty, or is the price of removing those contractual safeguards too high?

C. *Are Smart Contracts a Good Thing?*

In what follows, I consider the benefits and risks to consumers of different types of transactional automation, in order to isolate those which concern negative automation. I shall leave to one side the problems that arise from uncertainties in legal classification;²²⁴ these problems arise wherever technology outpaces legal evolution. I argue in what follows that the problems smart contracting seeks to solve are largely illusory, and that the harms (an increased vulnerability to fraud and hacking, and a lack of remedial recourse) are real and serious.

1. Positively-Automated Contracts

There are various ways in which contractual agreement and performance may be automated. Some of those methods are digital: infrastructure, education, utilities, and commerce all rely upon a nuanced network of self-operating, interdependent computer processes. This sort of automated contractual performance is commonplace, and it is crucial to much of what we do on a day-to-day basis.²²⁵ I may also bind myself digitally to create a future agreement: if I enter a maximum eBay bid, I thereby trigger a program that will enter a bid on my behalf if I am outbid.²²⁶ Some of those methods are contractual: when the end of the initial term of a tenancy agreement or gym contract arrives, the

²²² Or simply on the basis of an ordinary causative mistake.

²²³ *Supra* note 206 and accompanying text.

²²⁴ Though these problems may have a significant impact on the capacity of the law to respond.

²²⁵ Whether, for example, travelling to work, buying coffee, or streaming media.

²²⁶ It is now well-documented that the so-called “Internet of Things” promises the ability to instantiate these sorts of agreements more broadly, allowing, for example, household devices to reorder goods in an automated fashion.

agreement will usually “roll over,” binding the parties to a month-by-month contract. Automatic agreement may shape the entire contractual arrangement, or it may shape only part of it: many service-providers require consumers to provide blanket consent to fundamental unilateral variations in price or service.

The efficiency gains of contractual automation are well-understood;²²⁷ many services would be wholly unworkable without it. But whenever consumers bind themselves to some future agreement, or otherwise give up control over some part of their contract, questions arise concerning the long-term impact of that arrangement. Free trials regularly seduce consumers to enter into contracts that they (legally or practically) cannot quit, and consumers often discover that they are bound to some contract that (as a result of some unilateral variation on the part of their service-provider) looks little like the one to which they originally agreed. Where the consumer is particularly vulnerable or occupies a bargaining position of relative weakness, this concern is aggravated.²²⁸

Moreover, the remedial consequences of performance can be automated in such a way as to tilt the balance of power between the parties.²²⁹ At the outset of this paper, I considered the example of an instalment-plan supported by a program that would transfer the car’s e-key to the owner if the buyer defaulted. Such an arrangement may be more efficient, but it places a great deal of power in the hands of the owner. The consequences of any (however small) delay in payment are stark and inevitable. The greater the importance of the asset to one’s personal life, the greater the impact of default.²³⁰

So, while self-operating machines form a crucial part of our lives, they also raise serious risks of harm. Those risks do not always elicit appropriate caution from consumers; Radin identifies a “heuristic bias” that tends to produce over-optimism when it comes to assessing contractual risk.²³¹ There have been a range of institutional responses to that heuristic bias;²³² those responses are more or less cognizant of the subtler ways in which consumers may be “nudged”²³³

²²⁷ See LESSIG, *supra* note 4; see also BARTLETT, THE DARK NET, *supra* note 45; BARTLETT, THE PEOPLE VS TECH, *supra* note 45; JARON LANIER, WHO OWNS THE FUTURE? (2014); JARON LANIER, YOU ARE NOT A GADGET: A MANIFESTO (2011).

²²⁸ See RADIN, *supra* note 158.

²²⁹ See, e.g., Werbach & Cornell, *supra* note 9, at 124–25 (“Networked door locks on a shared car [through a system] such as Zipcar could automatically open, but only for that individual, that paid the access fee. Or, a lessor could shut off a delinquent lessee’s access to a leased car, and give access to the bank, but only until full payment of the principal.”).

²³⁰ One might imagine a mortgage agreement for a house on such terms; the impact of default would leave an individual homeless.

²³¹ RADIN, *supra* note 158, at 26–29.

²³² From regulating actors directly and enhancing consumer recourse to supporting competitors via accelerator programs.

²³³ I mean this in the technical sense. See, e.g., RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2009) (“A nudge, as

towards particular actions that may enable them to exercise meaningful control over contracts.

Let us turn, now, to the benefits and risks created by the ability to access contractual structures that, by relying upon persistent script, *preclude* either party from interfering with contractual performance.

2. Negatively-Automated Contracts

Above, I identified two features that set the vending machine apart from an automated asset-transfer program: First, confidence in counter performance does not depend upon the reputation of any particular counterparty; and, second, sale can be executed without intermediaries at the point of purchase. By placing operational control outside the hands of any individuals, smart contracting removes these differences. Yet, shifting trust from one's counterparty to a (digital or physical) machine is an advantage to the consumer only if three propositions are true: first, counterparties and intermediaries do not *warrant* one's trust; second, the machine *does* warrant trust; and, third, there are no other downsides that might outweigh the advantages of negative automation.²³⁴ Let us start with the first proposition.

The question of trust is fundamentally context sensitive. In Episode 76 of *Blockchain Insider*,²³⁵ Vitalik Buterin posits a scenario in which the auction host of a platform like eBay colludes with a seller to artificially inflate the price of an asset. The host has access to all maximum bids and might (Buterin imagines) "bid up" an asset. Buterin argues that Ethereum, by precluding such interference, offers greater transparency and reliability.²³⁶ He imagines a two-stage model: at stage one, everyone publishes invisible commitments to bid; at stage two, those bids are revealed.²³⁷

There are, of course, clear advantages to sellers in having the capacity to manage the auction in a more nuanced way, and there are clear advantages to both parties in having recourse to the platform in the event of questions or concerns. The question is whether there is a sufficient risk of manipulation that

we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not.")

²³⁴ Werbach asks:

[W]hat needs does the blockchain address, either for the first time or in new ways? . . . The benefits of these systems come with significant costs, not least of which are their novelty and immaturity. If an existing technology can do the same thing, it is likely to be the better approach.

WERBACH, *supra* note 17, at 73.

²³⁵ *Ep. 76. Vitalik Buterin*, BLOCKCHAIN INSIDER (Dec. 13, 2018), <https://bi.11fs.com/78>.

²³⁶ *Id.*

²³⁷ *Id.*

buyers would prefer Buterin's disintermediated model—or in other words, whether platforms *do* set out to defraud their buyers.

By and large, the answer to that question will be no; the reputational costs of mismanagement are far too high. This is more obviously true wherever there exists a strong supportive system of regulatory oversight. And if the answer is no, there is very little to be gained by designing contracts in such a way as to preclude this sort of intermediation. But let us assume, *arguendo*, that there are exceptions to that conclusion—that there are enough nefarious commercial actors, supported by weak regulatory oversight, for consumers to wish for a real alternative. The question, then, is whether blind consensus platforms offer a *more* trustable alternative?

One method for upsetting the otherwise-predictable outcomes of smart contracts concerns hacking. Malicious computer hacking is the exploitation of some loophole in the code of a particular program or application in order to execute a function that was not intended by the program's creators.²³⁸ Whenever computers carry out commercial activity, there is always a risk of this sort of interference, but commercial and governmental bodies have sufficient resources to build systems that are immune to most attacks, can respond quickly to any attack that does occur, and have deep enough pockets to compensate consumers from any untoward effects. Those who build applications on blind consensus protocols do not generally have access to an equivalent breadth and depth of financial and technological resource. We have already witnessed one fairly catastrophic impact of this problem, in the context of the DAO heist.²³⁹

Of course, we also saw how the community responded to that attack: enough miners implemented the software update to provide a new chain, which restored the funds to the DAO and allowed them to be recovered by users.²⁴⁰ There are reasons to applaud Ethereum's community for reaching a solution, but there are also reasons for worrying about the way in which it was reached. In particular, the method (a great deal of informal discussion on online fora)²⁴¹ is far too cumbersome to be implemented in the vast majority of cases. Moreover, the solution was altogether *ad hoc*. Nothing is assured by way of systematic remedial capability, and there are no formal systems of government to implement such capability.²⁴²

²³⁸ *Hacking*, TECHOPEDIA, <https://www.techopedia.com/definition/26361/hacking> (last visited Sept. 29, 2019) ("Hacking generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.").

²³⁹ The DAO hack ran into several million dollars, and substantially shook confidence in the Ethereum network. See *supra* notes 178–182 and accompanying text.

²⁴⁰ *Id.*

²⁴¹ Finley, *supra* note 178.

²⁴² On the governance question, see Vitalik Buterin, *Notes on Blockchain Governance*, VITALIK BUTERIN (Dec. 17, 2017), <https://vitalik.ca/general/2017/12/17/voting.html>; Vili Lehdonvirta, *The*

This is not the first time these questions of self-government have arisen. In 1999, Lawrence Lessig described LambdaMOO, a text-based virtual reality world.²⁴³ One of the players, “Mr_Bungle,” developed the ability to co-opt the voices and actions of other characters.²⁴⁴ The player used this power to violate those characters, and to make it appear that they were enjoying the experience.²⁴⁵ The community response was one of outrage.²⁴⁶ When the creators of the game (the “Wizards”) refused to intervene, some of the players met to discuss the matter in a virtual forum.²⁴⁷ Eventually, one of them took matters into his own hands, deleting the account associated with Mr_Bungle.²⁴⁸ Lessig wrote that “[t]here is a certain romance tied to the idea of [this sort of] democracy,” but “LambdaMOO’s move to self-government, through structures of democracy, was not just an achievement. It was also a defeat. The space had failed. It had failed, we could say, to self-regulate.”²⁴⁹

These criticisms are just as apt for Ethereum, though the nature of blockchain technology tends to obscure the processes of government.²⁵⁰ Of course, those who contribute to (by writing, by implementing, or otherwise by influencing) the code of blind consensus platforms could come up with more robust, systematic methods of self-government. However, these communities have expressed a strong and growing commitment to “immutability,”²⁵¹ promoting the indelibility of transactions and freedom from government, anarchy, not technocracy.²⁵² It now seems likely that a large-scale hack would elicit no solution at all, *ad hoc* or otherwise.

So, blind consensus platforms increase vulnerabilities to hacking and offer fewer opportunities to resolve problems that may arise as a result of

Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy, OXFORD INTERNET INST. (Nov. 21, 2016), <https://www.oii.ox.ac.uk/blog/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy/>; Vlad Zamfir, *Against On-Chain Governance Refuting (and Rebuking) Fred Ehrsam’s Governance Blog*, MEDIUM (Dec. 1, 2017), https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca.

²⁴³ LESSIG, *supra* note 4, at 74–78.

²⁴⁴ *Id.*

²⁴⁵ *Id.*

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ *Id.*

²⁴⁹ *Id.* at 77.

²⁵⁰ See Lehdonvirta, *supra* note 242.

²⁵¹ See *supra* notes 178–180 and accompanying text.

²⁵² But see Mike Hearn, *The Resolution of the Bitcoin Experiment*, MIKE’S BLOG (Jan. 14, 2016), <https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7>.

hacking.²⁵³ In this sense, they are *less* trustable than their intermediated alternatives. Finally, let us turn to the third question: in what follows, I consider whether there are any (other) downsides to negative automation, which outweigh the putative benefits.

We have already seen that, even if one can have confidence that code will execute as it has been set up, there are still very many things that may go wrong with a coded contract. One party may act fraudulently or unconscionably, or one or more of the parties may be mistaken about the contract itself, or the conditions in which it is to be performed.²⁵⁴ The legal system offers a variety of remedial mechanisms. Some (we have seen) permit parties to return themselves to the nearest approximation of the position in which they were prior to the contract. Others allow the parties to set aside or otherwise adjust unfair contract terms.²⁵⁵

This formal architecture is supported by a variety of powerful and flexible non-law mechanisms. Some of those mechanisms are prophylactic: security enhancements in banking protect consumers from fraudsters, and a screening process is conducted by companies such as Uber, Airbnb, and Amazon to ensure that consumers are not exposed directly to harmful actors. Some of those mechanisms are remedial: each of these companies provides compensation in the event that a wrongful transaction does occur. There are many reasons to think that consumers value this remedial infrastructure a great deal,²⁵⁶ and that the ability to enter into contracts that *absorb risk* is an asset.

It bears emphasis that these intermediaries often offer a solution, not because of any legal obligation, but because they wish to establish or maintain a particular *reputation*. Banks are not obliged to, but often will, recover funds paid by mistake; Amazon is not obliged to, but often will, refund the price of

²⁵³ See Bruce Schneier, *There's No Good Reason to Trust Blockchain Technology*, WIRED (Feb. 6, 2019, 9:00 AM), <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/> (“What blockchain does is shift some of the trust in people and institutions to trust in technology. You need to trust the cryptography, the protocols, the software, the computers and the network. And you need to trust them absolutely, because they’re often single points of failure. When that trust turns out to be misplaced, there is no recourse. . . . In many ways, trusting technology is harder than trusting people. Would you rather trust a human legal system or the details of some computer code you don’t have the expertise to audit?”).

²⁵⁴ Moreover, a substantial imbalance in the relative bargaining position of the parties may produce a set of terms that prejudice the weaker party.

²⁵⁵ Here, different jurisdictions produce different answers. The U.S. has a doctrine of unconscionability. *See, e.g., Williams v. Walker-Thomas Furniture Co.*, 350 F.2d 445 (D.C. Cir. 1965). On the other hand, the UK has narrower doctrines of duress and undue influence, and the statutory framework embodied in the Unfair Contract Terms Act 1977 (Eng.).

²⁵⁶ Stinchcombe, *Ten Years In*, *supra* note 67 (“With all the money spent on bitcoin cash registers, nobody went out and did a survey about whether most credit card users would be willing to give up their frequent flyer miles in return for also losing the ability to dispute a transaction.”). It is worth noting that very many so-called blockchain-based applications in fact rely on intermediaries. *See WERBACH, supra* note 17, at 74.

marketplace goods that do not meet the buyer's expectations. In this sense, the trust that one places in an intermediary—far from acting as a disadvantage—can be an invaluable bargaining chip.

We have seen that smart contracts preclude access to much of this remedial infrastructure.²⁵⁷ Parties who transact on a peer-to-peer basis must rely on the cooperation of their counterparty in the event of any mishap in contract or code formation. Parties who cannot identify their counterparty cannot sue to enforce that cooperation at all.²⁵⁸ Without the many safeguards implemented by traditional intermediaries, parties are more exposed to harm, and without the remedial mechanisms of intermediation, most parties will be wholly unable to fix that harm.

Here, limits in programmatic capability bite with particular ferocity. Recognizing the possibility of the kinds of problem under consideration here, Szabo argued that certain “hardship and operational” controls might usefully be “coded in” to smart contracts.²⁵⁹ It is not altogether clear what he meant by this, and there are good reasons why these sorts of controls have not emerged. Not only is it extremely difficult to identify in advance all of the events that might frustrate the parties' plans, the question of whether someone's intention was in fact impaired at the time of contract formation is a question poorly-suited to resolution by computer code.²⁶⁰

There are, in sum, good reasons for consumers to *prefer* to place trust in cognizable counterparties and intermediaries, where these actors are able to insure against the very many ways in which a contract may go wrong. Rather than trying to remove trust from digital commerce, we might better focus our

²⁵⁷ See DE FILIPPI & WRIGHT, *supra* note 8, at 85 (“[R]obust common law and civil law doctrines—such as unconscionability and incapacitation—soften the blow of contracts that contain lopsided or unfavorable terms. In the context of smart contracts used to govern transactions between pseudonymous parties, however, injured parties likely will lack the ability to rely on these defenses, possibly encouraging the deployment of smart contract-based agreements that disproportionately favor parties with greater bargaining power.”).

²⁵⁸ Organizations that are not directly within the control of any definable group of individuals (such as the DAO) cannot easily be subjected to the regulatory oversight of any one national Government.

²⁵⁹ *Smart Contracts*, *supra* note 7.

²⁶⁰ These questions are best suited to human judgment. See DE FILIPPI & WRIGHT, *supra* note 8, at 84 (“Smart contracts are not particularly well suited to accommodate legal arrangements that are relational in nature. To implement a smart contract, parties need to precisely define performance obligations . . . in many commercial transactions . . . obligations will likely prove unpredictable, and smart contracts will not be able to provide parties with the flexibility to structure their ongoing contractual relationships.”). Parties *could* specify a mutually trusted decision-maker—but that serves to reintroduce precisely the possibility of intermediation that blind consensus protocols are designed to oust.

efforts upon mechanisms for making sure that that trust is well-placed.²⁶¹ We have seen that there is a great deal of value to consumers in the ability to see and influence a company's reputation.²⁶² We ought to encourage, not eliminate, this sort of method for improving transparency and accountability with respect to a company's commercial practices.²⁶³

At this juncture, I will express two predictions and one hope for the future of digital contracting. The first prediction is that centralized and intermediated mechanisms of contracting will prevail. We have already seen that negative automation is extremely cumbersome.²⁶⁴ And we have also seen that there are good reasons for companies to wish to retain control over their contracts.²⁶⁵ If they rely upon shared programs and records, it will be in the context of permissioned protocols; they will not use a wholly-open process of transaction verification.²⁶⁶

The second prediction is of an even greater shift to standardizing contracts. This is sometimes expressed as "modularity."²⁶⁷ That, in turn, is presented as an advantageous feature for consumers and small businesses.²⁶⁸ The claim is that traditionally weaker parties may select their contractual text (without recourse to lawyers).²⁶⁹ Yet, more modularity does not entail greater choice for consumers. The phenomenon of "boilerplate contracts" shows that companies may present the contractual text as a *fait accompli*.²⁷⁰

The hope is that we will design our contractual systems to accommodate imperfect rationality, foresight, and bargaining power. This, of course, means regulating providers to ensure that consumers are given opportunities to exercise meaningful control over their contracts. But it also means encouraging those who seek to develop technologies that challenge the incumbent commercial

²⁶¹ As Kai Stinchcombe puts it in Stinchcombe, *Blockchain*, *supra* note 67, "[i]nstead of directing resources to the *elimination* of trust, we should direct our resources to the *creation* of trust."

²⁶² In this sense, models of commerce that encourage pseudonymous or anonymous contracting lack a valuable resource.

²⁶³ Some of these methods are legal; others are not. Systems of open review, which crowdsource information, establish clear pictures about which commercial actors are worthy of trust.

²⁶⁴ Proof of work is designed to be computationally intensive.

²⁶⁵ Stinchcombe, *Ten Years In*, *supra* note 67.

²⁶⁶ This prediction holds for both consumer and (higher-value) commercial contracts.

²⁶⁷ See DE FILIPPI & WRIGHT, *supra* note 8, at 80–83.

²⁶⁸ *Id.*

²⁶⁹ *Id.*

²⁷⁰ Nor does it necessarily entail less reliance on lawyers: like any other intermediary, a lawyer is able to ensure the party against risk. Someone very well versed in property law and conveyancing will ordinarily employ a lawyer to conduct the process simply so that they have an avenue of recourse if something goes wrong.

infrastructure to think seriously about questions of ethics and (to that end) government. We saw at the very outset of this article that the goals of this experiment in contractual technology were to improve transparency and accountability.²⁷¹ Those are proper goals, but they should be stepping stones towards a system that promotes trust. Better accountability ensures that commercial actors behave in a more trustworthy fashion. More transparency equips consumers to choose commercial actors that act in a trustworthy fashion. A utopian future of commerce is not one in which consumers are held to degenerate contracts; it is one that supports valuable relationships of trust and cooperation.

IV. CONCLUSION

The evolution of contracting is rarely presented as a story of consumer empowerment. Rather, commentators emphasise the proliferation of mechanisms that place control firmly in the hands of the party with the most commercial clout.²⁷² The phenomenon of smart contracting is supposed to buck that trend. By immunizing contracts from operational interference, smart contracts carve out a domain free from political and commercial influence.²⁷³ That sentiment ought to be understood in context. Bitcoin was built in the wake of the 2008 financial crisis, when faith in financial intermediaries was at its lowest ebb. But I have demonstrated that there is a substantial cost to removing these intermediaries—and that cost is borne by consumers.

In Part II of this article, I explained how smart-contracting works, and how it differs from existing tools for digital commerce. The crux of that difference is the ability to take operational control out of the hands of powerful counterparties and intermediaries. The problem smart-contracting sets out to solve is the need to make digital contracts tamper-proof. And the “core case” of a smart-contract is the solution—computer code that negatively automates contractual performance. In Part III, I argued that negative automation does not enhance consumer autonomy, nor make for better bargains. The ability to escape from contracts in certain circumstances is a core part of the law’s commitment to supporting valuable relationships of trust and reliance. By obviating “thick” trust,²⁷⁴ and removing contractual safeguards, smart-contracts increase the likelihood that parties will be bound inexorably to contracts that are wholly lacking in the relational virtues supported by the law of contract.

²⁷¹ *Supra* notes 39–41 and accompanying text.

²⁷² *See* RADIN, *supra* note 158.

²⁷³ I put this in terms of “negative automation” and non-justiciability; the idea is that neither intermediaries nor contracting parties can interfere with performance—during performance or after.

²⁷⁴ Parties have a general confidence that their counterparty’s intentions conform to their outward manifestation. *See supra* note 220 and accompanying text.

When Lessig wrote his oft-quoted statement that “code is law,”²⁷⁵ he did not argue that code should *replace* normative questions; quite the opposite. He argued that those who built spaces for online interaction could choose to design their code “to protect values that we believe are fundamental” or could “allow those values to disappear.”²⁷⁶ As the computer sciences grow, so too must the clamour of social scientists—that these values become a core part of technological ambition.

²⁷⁵ LESSIG, *supra* note 4.

²⁷⁶ *Id.* at 6.

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:

Cutts, T

Title:

Smart Contracts and Consumers

Date:

2019-01-01

Citation:

Cutts, T. (2019). Smart Contracts and Consumers. SSRN Electronic Journal, 122 (2), pp.389-445. <https://doi.org/10.2139/ssrn.3354272>.

Persistent Link:

<http://hdl.handle.net/11343/260440>