

9-2014

Smart Contracts, Bitcoin Bots, and Consumer Protection

Joshua A.T. Fairfield

Washington and Lee University School of Law, fairfieldj@wlu.edu

Follow this and additional works at: <http://scholarlycommons.law.wlu.edu/wlulr-online>



Part of the [Banking and Finance Commons](#)

Recommended Citation

Joshua A.T. Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 36 (2014), <http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3>

This Round table: Crypto-Currency 2.0 is brought to you for free and open access by the Law School Journals at Washington & Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review Online by an authorized administrator of Washington & Lee University School of Law Scholarly Commons. For more information, please contact osbornecl@wlu.edu.

Smart Contracts, Bitcoin Bots, and Consumer Protection

Joshua Fairfield*

Abstract

Trustless public ledgers (“TPLs”)—the technology underneath Bitcoin—do more than just create online money. The technology permits people to directly exchange money for what they want, with no intermediaries, such as credit card companies. Contract law is the law of bargained-for exchange, so a technology that enables direct exchange online will change the reality of online contracting. The current problem with consumer contracting online is that courts and companies have collaborated to create an online system in which consumers cannot bargain. Under the current regime, consumers have no choice but to click the “I Accept” button. Online, contract law is not the law of bargained-for exchange; it has become the law of company-dictated exchange. Smart contracts—automated computer programs able to execute trades through TPLs—may offer a solution. This brief Essay explores the possibilities of smart contracts and their potential to correct the badly off-course law of online contract.

Table of Contents

I. Introduction	36
II. Radical Disintermediation.....	40
III. Consumer Contract Exclusion.....	41
IV. Automated Agents and Consumer Protection.....	44

* Joshua Fairfield is a Professor of Law at the Washington and Lee University School of Law. He is a nationally recognized scholar on law, governance, economics, and intelligence issues related to technology. Thanks to Lindsey Jones, Joshua Deal, Krystal Swendsboe, and Alex Flachsbart for their assistance with researching and editing this Essay.

V. Challenges to Consumer-Originated Smart Contracts.....	46
VI. Conclusion.....	49

I. Introduction

Trustless public ledgers are online lists, maintained by no one and available to everyone, that are maintained by a consensus protocol.¹ For example, imagine a list on a whiteboard in a dormitory floor, keeping track of who paid for pizza last time. The advantages to such a list—public availability and ease of editing—are clear. The disadvantages are equally clear. Someone might attempt to edit the list to their personal advantage. A solution that immediately suggests itself is that the dorm RA might be entrusted to keep the list. Yet then there is the concern that the RA may make a mistake, or be unavailable over the weekend, or be untrustworthy and edit the list to benefit himself. What is needed is a public ledger that is constrained by rules of consensus to prevent individuals from modifying the list to their exclusive benefit. That is the central technology underlying Bitcoin: the “trustless public ledger” (TPL).² The ledger is public because anyone can download a copy.³ It is trustless because the underlying mathematical rules make it extraordinarily difficult to unilaterally change the list in the face of an opposing consensus.⁴ It is

1. See Barrett Sheridan, *Bitcoins: Currency of the Geeks*, BLOOMBERG BUSINESSWEEK (June 16, 2011), http://www.businessweek.com/magazine/content/11_26/b4234041554873.htm (last visited July 31, 2014) (describing the communal verification process for Bitcoin transactions) (on file with the Washington and Lee Law Review).

2. See Paul H. Farmer, Jr., *Speculative Tech: The Bitcoin Legal Quagmire and the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 89 (2014) (explaining how public Bitcoin recordkeeping permits transactions without third party oversight).

3. See *id.* (describing the type of electronic ledger used in Bitcoin transactions); Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 116 (2012) (describing the public nature of Bitcoin transactions).

4. See Farmer, *supra* note 2, at 89 (describing the “cryptographic proof” of transactions maintained in the ledger, which are designed to remove third parties’ ability to manipulate transactions).

disintermediated because no single entity can control or manipulate the list.⁵ Entrepreneurs and analysts agree that TPLs—of which Bitcoin is merely one example⁶—can potentially restructure the power relationship between consumers and intermediaries online.⁷ Because the Bitcoin block-chain protocol is strongly disintermediated, intermediaries lose some of the pride of place that they enjoyed in the online economy as it evolved over the past twenty years.⁸

The rhetoric of Bitcoin enthusiasts is overblown, but contains a kernel of truth. Although TPLs will not cause internet intermediaries to wither away, they will cause a shift in the balance of power between consumers and intermediaries.⁹

5. See *id.* at 89–90 (explaining how each transaction requires information (the public and private keys) from both the buyer and seller, which is recorded in the transaction data and cannot be altered by one person).

6. See John Evans, *Bitcoin 2.0: Unleash the Sidechains*, TECHCRUNCH (Apr. 19, 2014), <http://techcrunch.com/2014/04/19/bitcoin-2-0-unleash-the-sidechains/> (last visited Aug. 5, 2014) (“Bitcoin is both the first and most successful blockchain application, but there are many, many other ‘cryptocurrencies,’ known as ‘altcoins.’”) (on file with the Washington and Lee Law Review).

7. See, e.g., Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 347–48 (2008) (providing one example of the disruptive power of public ledgers that allows capital to be used to develop new services such as the elimination of transaction costs); Perianne Boring, *BitGo Raises \$12Mil, Draws Attention of Institutional Investors*, FORBES (June 16, 2014), <http://www.forbes.com/sites/perianneboring/2014/06/16/bitgo-raises-12mil-draws-attention-of-institutional-investors/> (last visited July 31, 2014) (discussing one innovation, multi-signature technology (“Multisig”), which gives parties using Bitcoin recourse in the case of the other party’s nonperformance) (on file with the Washington and Lee Law Review); John Villasenor, *Could ‘Multisig’ Help Bring Consumer Protection to Bitcoin Transactions?*, FORBES (Mar. 28, 2014), <http://www.forbes.com/sites/johnvillasenor/2014/03/28/could-multisig-help-bring-consumer-protection-to-bitcoin-transactions/> (last visited July 31, 2014) (describing Multisig’s effects on markets using Bitcoin) (on file with the Washington and Lee Law Review).

8. See Kaplanov, *supra* note 3, at 116 (describing public ledger systems, specifically Bitcoin transactions, as “free of third party presence—whether that third party is a government, bank, payment network, or clearinghouse. . . . [This] allows parties to the transaction to deal directly with one another without a third party authorizing the transaction”).

9. See *supra* note 7 and accompanying text (describing one innovative service, Multisig, where third parties will continue to be relevant because they serve as custodians, ensuring both parties to a transaction perform their obligations).

Consumers may still find it useful to use bank-like institutions. Yet they need not. The trustless ledger system permits them to transfer and hold money in large amounts on their own account.¹⁰ The question is whether TPLs will have a similar effect in other areas of law outside of the financial sector.¹¹

What has until now flown under the radar is the fact that Bitcoin is merely the tip of an iceberg. Given the speed with which new business models are developing around crypto-currencies and trustless technologies,¹² it is time to start looking past routine financial applications of such ledgers as currencies. They do much more. TPLs permit parties not only to hold digital assets of value without banking intermediaries; they also permit parties to transfer digital assets of value directly, on their own terms, without any institution acting as an exchange intermediary.¹³

Smart contracts—automated programs that transfer digital assets within the block-chain upon certain triggering conditions¹⁴—represent a new and interesting form of organizing

10. See Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled Onto Something Much, Much Bigger*, BUSINESS INSIDER (Apr. 22, 2014), <http://www.businessinsider.com/the-future-of-the-blockchain-2014-4> (last visited Aug. 4, 2014) (describing how block-chain security permits individuals to verify transactions and property's existence, therefore assuring market participants of the safety of the block-chain-based digital marketplace) (on file with the Washington and Lee Law Review).

11. See *id.* (speculating as to whether groups such as BitShares and Ethereum will succeed in efforts to implement block-chain technology in areas such as stock exchanges, voting, and music distribution).

12. See EUROPEAN CENTRAL BANK, VIRTUAL CURRENCY SCHEMES 16–18 (2012), <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> (describing the plethora of virtual currencies from the Linden Dollar to Bitcoin and the services that accompany them, including Paypal).

13. See Wile, *supra* note 10 (“[TPLs have] no intermediaries, therefore there’s really nothing to stop a computer from just connecting to the Internet and taking part all by itself. All you need to do to instantiate a Bitcoin wallet is generate a large random number.” (quoting an interview with Mike Hearn)); *supra* note 8 and accompanying text (describing public ledgers as being virtually free of intermediaries).

14. See David Morris, *Bitcoin Is Not Just Digital Currency. It's Napster for Finance.*, FORTUNE (Jan. 21, 2014), <http://fortune.com/2014/01/21/bitcoin-is-not-just-digital-currency-its-napster-for-finance/> (last visited Aug. 5, 2014) (defining smart contracts and providing examples such as a car that would automatically disable itself if loan payments were not made) (on file with the Washington and Lee Law Review).

contractual activity. If financial transactions can be freed of banks as intermediaries, then contracts can be freed of courts as intermediaries. This solves a longstanding puzzle and problem of e-commerce: courts' longstanding refusal to enforce contract terms proffered by consumers.¹⁵ If courts will not protect consumers, robots will.¹⁶ Consumers can use automated consumer-grade purchasing agents, tied to Bitcoin wallets and preprogrammed with consumer preferences, to reclaim their ability to negotiate in online transactions.

This Essay proceeds as follows. Part II briefly discusses how TPLs disintermediate online exchange, and further describes how exchange disintermediation can lead to a revitalization of consumers' ability to offer, enter into, and enforce contracts online. Part III discusses the phenomenon of online consumer contract exclusion, and explores why consumer-proffered contract terms are denied enforcement in e-commercial arrangements. Part IV focuses on how Bitcoin-fueled smart contracts can be used by automated software agents to protect consumers' identity from theft and automatically enforce their contractual preferences. Part V discusses and engages the standard challenges to consumer-oriented theories of online contract.

15. See, e.g., James Gibson, *Vertical Boilerplate*, 70 WASH. & LEE L. REV. 161, 167–69 (2013) (noting that the modern marketplace relies on competition to weed out onerous contracting terms, rather than consumer negotiation); *id.* at 170–80 (explaining why the idealized compensatory model does not work with boilerplate contract language in the modern marketplace); Cheryl B. Preston & Eli W. McCann, *Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse*, 26 BYU J. PUB. L. 1, 23 (2011) (explaining how online service providers often do “not allow the consumer the same luxury of changing the contract at will, but instead retains the unilateral modification power exclusively for itself”); *id.* at 23–28 (exploring the legal sacrifices that consumers make when contracting with online service providers—a completely asymmetric contract relationship); see also Joshua Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047, 1071–72 (2005) (describing traditional limits on contract enforceability, including limits on use and locking-in low-value property uses).

16. See Morris, *supra* note 14 (explaining that, because Bitcoin is entirely distributed, the system permits “loans without banks, contracts without lawyers, and stocks without brokers, executed and recorded across hundreds of servers at all corners of the earth”).

II. Radical Disintermediation

TPLs disintermediate exchange.¹⁷ They permit parties to transmit money or other valuable online assets to one another securely and cheaply, without relying on any centralized entity to curate a database of who owns what.¹⁸ Previous systems for digital money have relied on a centralized list curator to control the list of which assets are ascribed to whom.¹⁹ Thus, to move a digital asset from Person A to B, one must contact the list curator, and have that person change the entry “Person A owns asset X,” to “Person B owns asset X.” The cost of the list curator and the chance that that curator may fail, mishandle, or manipulate the list, are all costs that must be borne by such systems.

TPL systems propose a solution to the problem of expensive intermediaries. They offer a consensus system for maintaining a decentralized list of who owns what.²⁰ The coordination problem is addressed by a proof-of-work system, which makes it expensive and difficult to compromise the list.²¹ This system scales elegantly: the more value that comes into the system, and the more people that seek it, the harder the system is to compromise.²²

A full discussion of the mechanics of Bitcoin is well beyond the scope of this short Essay, and much has already been written. What is important to take away is that Bitcoin innovates in two ways. It is a method for tracking who owns which property

17. See Kaplanov, *supra* note 3, at 125–26 (explaining Bitcoin’s ability to eliminate intermediaries as necessary parties to transactions).

18. See *id.* at 127–28 (discussing how Bitcoins are used to get around traditional methods of blocking money transfers, and how some people treat Bitcoins as an investment).

19. Cf. *supra* note 7 and accompanying text (describing one innovative service, Multisig, where third parties will continue to be relevant because they serve as custodians, ensuring both parties to a transaction perform their obligations).

20. See Evans, *supra* note 6 (describing TPLs and block-chain technology as “a peer-to-peer network . . . used to codify and cryptographically verify transactions, without any central authority”).

21. See Morris, *supra* note 14 (explaining the proof-of-work system as constant vetting of transactions by a “vast network of ‘miners’ rewarded for their maintenance work with a stream of bitcoin”).

22. See Sheridan, *supra* note 1 (illustrating the miners’ work and how larger numbers and processing power allow for a more secure TPL).

interests without a centralized intermediary, and it is a method for transferring that property directly, peer to peer.²³ The second characteristic has further ramifications. If consumers can now make disintermediated property or currency exchanges, then they can begin to make disintermediated contractual arrangements.²⁴ If consumers can hold money without banks, they can enforce contracts without courts.²⁵ If consumers can offer their own standardized contractual agreements, then they may be able to undo the radical disenfranchisement of consumers in online contracting environments.

III. Consumer Contract Exclusion

This Essay supports its argument that courts prevent consumers from enforcing expressed online contractual terms through a thought experiment. Consider and compare the following scenarios. First, a consumer logs onto a corporate web server, seeking to buy a widget. She encounters there contractual terms and conditions, which she clicks through without reading (although she has a rough idea what is in them), and concludes a purchase. The contract is enforceable according to its terms.²⁶

Second, a software agent logs into a corporate web server. The computer program encounters various terms and conditions, either because of an electronic data interchange²⁷ format (for business-to-

23. See Morris, *supra* note 14 (illustrating both direct property transfers and the public tracking of transfers within a TPL network).

24. See *id.* (describing property relationships that would be enabled with Bitcoin technology, including managing real-world leases and entering into mortgages and purchase contracts).

25. See *id.* (giving one example: the ability to enforce car payments).

26. See Mark Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 466 (2006) (stating that every court that has considered the validity of shrink-wrap contracts has held them valid and binding); Rachel Conklin, *Be Careful What You Click For: An Analysis of Online Contracting*, 20 LOY. CONSUMER L. REV. 325, 327 (2008) (“Clickwrap contracts have been accepted as valid by United States courts virtually every time they have been challenged.”).

27. An electronic data interchange is “the computer-to-computer exchange of business documents in a standard electronic format between business partners.” *What is EDI (Electronic Data Interchange)?*, EDI BASICS, <http://www.edibasics.com/what-is-edi/#sthash.pMY8jxXo.dpuf> (last visit Aug. 29,

business purchases), or because it runs into some other machine-readable text, such as a robots.txt file (for web crawlers and indexing agents). The machine concludes a purchase. The contract is enforceable according to its terms.²⁸

Third, a consumer's software agent logs into a corporate web server. The consumer's software agent offers specific contractual terms stating the terms on which the consumer is willing to deal. For example, the consumer may have informed the web server that she is only willing to deal with that server if the server respects her desire not to sell her personal data, by setting a "do not track" flag.²⁹ The corporate web server, having been apprised of those terms but programmed to take no notice of them, concludes a purchase anyway. The consumer contract is not enforceable according to its terms.³⁰

Why? Somewhere in the shift from dickered, black letter law-negotiated contracting to non-dickered, standardized, mass-market consumer contracting, the ability of consumers to negotiate their own contract terms vanished.³¹ Under sustained assault by

2014) (on file with the Washington and Lee Law Review). A "computer-to-computer" transaction means that "EDI documents can flow straight through to the appropriate application on the receiver's computer (e.g., the Order Management System) and processing can begin immediately" without involving paper or people. *Id.*

28. See, e.g., NEV. REV. STAT § 719.310 (2001) ("A contract may be formed by the interaction of electronic agents of the parties, even if no natural person was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.").

29. A "do not track" flag is a browser setting that allows consumers "to choose whether they want to allow websites to collect information about their Internet activity and use it to deliver targeted advertisements and for other purposes." *Do Not Track*, FED. TRADE COMMISSION, <http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track> (last visited Aug. 30, 2014) (on file with the Washington and Lee Law Review).

30. See Lemley, *supra* note 26, at 464 (describing the battle of the forms and noting that when a contract features conflicting forms, the conflicting terms are read out of the contract unless one party has demonstrated a willingness to forgo the deal over that term); Ian Rambarran & Robert Hunt, *Are Browse-Wrap Agreements All They Are Wrapped Up To Be?*, 9 TUL. J. TECH. & INTELL. PROP. 173, 201 (2007) (arguing that implied consent to privacy terms can be created by browse-wrap agreements).

31. See Conklin, *supra* note 26, at 329–30 (explaining that, when interpreting browse-wrap contracts, courts generally find that a user's acceptance is implied by his or her use of a website); Lemley, *supra* note 26, at 470–71

courts and legal theorists, a consumer's ability to proffer legally binding online contractual arrangements has almost disappeared.³²

This state of affairs is fact, but has no basis in law. Courts do not enforce consumer-proffered online terms as enforceable contractual terms,³³ but they also do not admit that this is what they are doing.³⁴ Courts instead exclude the consumer preference from the four corners of the online agreement.³⁵ What the company wrote is "the contract," and the expression of consumer preference is simply not part of that contract.³⁶ Courts manipulate the contours of the contractual agreement to exclude expressions of consumer preference in online agreements.³⁷ If, however, consumers were able to somehow express their preferences unmistakably within the contours of what courts consider to be the online agreement, then courts would have no choice but to recognize consumer-proffered online contract terms.³⁸ Instead of just clicking "I Agree," consumers could actually contract again.

(explaining that judicial interpretation of browse-wrap contracts is based on traditional trespass: domain owners need only give notice that "trespassing" on their website is conditioned by contract terms in order to enforce their property rights).

32. See *supra* note 30 and accompanying text (demonstrating how, when a website user has a form contract or terms that are not explicitly accepted by the other party and the website user continues to use the website, the user's terms are read out of the contract and are not binding).

33. See *supra* note 30 and accompanying text (explaining that consumer-proffered online contract terms are unenforceable under current "battle of the forms" jurisprudence).

34. See *infra* note 35 (describing the factors courts purportedly consider).

35. See Rambarran, *supra* note 30, at 186 (describing three factors courts look at when analyzing browse-wrap contracts: notice, consent, and whether the substantive requirements for the particular terms were met).

36. See *supra* note 30 and accompanying text (explaining that consumer-proffered online contract terms are read out of a contract when there is a battle of the forms).

37. See Lemley, *supra* note 26, at 472–77 (describing courts' willingness to enforce browse-wrap terms against business consumers and concluding that courts are more willing to enforce retroactive amendments to contracts without consent and other anti-consumer terms in the business-to-business context).

38. See *id.* at 464 (arguing that a parallel interpretive canon to the "battle of the forms" for online business-to-business contracting would allow additional consumer power).

This is why e-commerce websites are so carefully engineered to limit any consumer expression of preference beyond quantity. When one shops at Amazon, one may pick the number of items shipped, but nothing else.³⁹ There is no drop-down box for consumer terms provided.⁴⁰ Consumers are constrained by the form of the webpage from offering other terms, such as reservations of rights and warranties.⁴¹ Consider the routine online disclaimer of warranties, which has eviscerated consumer protections offered by the Uniform Commercial Code.⁴² Some consumers may wish to pay more and refuse the disclaimer of warranty. Indeed, the Code system is so structured that if one party disclaims warranties, and the other requires those warranties, then the warranties exist.⁴³ Yet in the online context, such a disagreement over warranties cannot happen.⁴⁴ There is no warranty drop-down box.

IV. Automated Agents and Consumer Protection

What is needed is a format in which consumers can express their preferences to automated agents (often termed “bots” or “robots,” despite the agents’ lack of physicality), and then expect their preferences to be enforced. If courts discriminate against consumer preferences in online contracting, consumers will need

39. See, e.g., *The Sopranos: The Complete Series*, AMAZON, http://www.amazon.com/Sopranos-Complete-Various/dp/B006CR2OOA/ref=sr_1_1?s=movies-tv&ie=UTF8&qid=1408632827&sr=1-1&keywords=sopranos+complete+series (last visited Aug. 21, 2014) (allowing a customer to choose the quantity she would like to order) (on file with the Washington and Lee Law Review).

40. See, e.g., *id.* (providing a single drop-down box for quantity).

41. See, e.g., *id.* (providing no functionality for consumers to propose additional terms).

42. See Rambarran, *supra* note 30, at 187–90 (discussing warranties and other consumer protection devices articulated in the Uniform Commercial Code).

43. See Lemley, *supra* note 26 (“[T]he Uniform Commercial Code (U.C.C.) resolved this ‘battle of the forms’ by adopting a compromise: if the terms conflict, neither party’s terms become part of the contract unless a party demonstrates its willingness to forego the deal over it.” (citing U.C.C. § 2-207(3) (2003))).

44. See *supra* notes 39–41 and accompanying text (describing consumers’ lack of options for online contracting).

to turn to automated agents to protect their contractual preferences.

Automated consumer-grade purchasing software is already in common circulation. Consider eBay “sniping” programs. These are programs that are set to auto-bid on an item, up to a certain price, with certain parameters involving speed of bid and time interval between bids. The purpose of the sniping program is to wait to bid up an item until the time of the item has nearly expired. EBay offers its own bid-up program, permitting buyers to make automated bids up to a given level, to resist sniping from outsiders.⁴⁵ Thus, these systems are not only extant, they are commonplace.

What is not yet commonplace is the use of automated consumer purchasing software on an internet-wide scale. One reason for this is the limits and variability of payment options. It is possible to find a program that could be given a consumer’s credit-card information and told to hunt for good deals, and such programs have indeed been floated. But the variation in payment formats and the cost and complexities of payment have stymied widespread use of consumer-grade automation software. The early 1990s hesitation to entrust websites with credit card data has become an early 2010s hesitation to entrust automation software with financial information. This is all the more the case because of identity fraud.

Yet, identity fraud is a byproduct of the locked-down financial e-commercial infrastructure within which consumers have been, until now, constrained to operate. Until recently, a party who wishes to pay for something online must reveal her personal information. This is because the nature of the transaction is contract-based, not property-based. An online payment is not a transfer of money from one person to another. It is, properly speaking, a chain of promises to pay. The credit card company settles with the bank of the vendor and receives payment in monthly installments from the consumer. For such a chain to function, each party must know the identity of the other parties in

45. See *Automatic Bidding*, EBAY, <http://pages.ebay.com/help/buy/automatic-bidding.html> (last visited Aug. 21, 2014) (describing eBay’s automatic bidding system, in which a customer may set a maximum bid and eBay will automatically increase the customer’s bid to maintain the highest bid up to the chosen maximum bid) (on file with the Washington and Lee Law Review).

the chain. A future promise to pay on the part of entity X is useless unless one knows X's identity.

Crypto-currency transactions, by contrast, permit consumers to buy items online without exposing their personal information. A consumer can transfer digital cash directly, instead of constructing a chain of identity supporting a promise of future payment. The vendor does not need to know who the buyer is, merely that the buyer can pay the amount of digital cash required. Consider the recent massive loss of credit card information by Target and other retailers during the 2013 holiday season.⁴⁶ Had those transactions been in Bitcoin, the consumers would have been as safe from identity theft as if they had paid in cash.

Automated software agents can be programmed with their own Bitcoin wallets, and can release funds, or not, according to consumer-set parameters. If companies do not satisfy the parameters, the deal does not go through. Consider a simple smart contract that a consumer instructs to buy a toaster. It is programmed to seek a single unit of the item, at the lowest price, and subject to a reservation of all rights and remedies, including all standard consumer warranties. The agent is connected to a Bitcoin wallet, and can therefore pay for the item without releasing the consumer's identity into the wild. Indeed, depending on the nature of the transaction and the need for shipping addresses, it is entirely possible that the agent can buy and sell on the consumer's behalf without providing any information about the consumer to the company at all.

V. Challenges to Consumer-Originated Smart Contracts

There are several challenges to this conception of smart contracts, automated agents, and consumer protection. Because these theoretical challenges represent the current received legal wisdom, they are briefly addressed and engaged here.

46. See *Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores*, TARGET (Dec. 19, 2013), <http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores> (last visited August 14, 2014) (confirming unauthorized access to more than forty million credit and debit card accounts) (on file with the Washington and Lee Law Review).

First, and most pragmatically, the technology is not shovel-ready. As futurist Clay Shirky has noted, technological revolutions do not get interesting socially until they are boring technologically.⁴⁷ Attempts to package and deliver consumer contractual preferences have foundered on whether the technology can operate smoothly.

Here, however, TPLs can play a large role in simplifying and enabling consumer-driven automated agents. The value proposition of TPLs is complicated, and the means by which the ledger itself is secured is a matter of moderately complex mathematics and some game theory. Yet the use of cryptocurrencies themselves is simple and could be even simpler. In particular, TPLs completely remove a major source of consumer hesitancy and complexity by eliminating the need for consumers to entrust automated agents with their personal information. A consumer setting up an autonomous agent would not even need to designate with whom the contract would be concluded. A price, a quantity, and warranties would do. The consumer can protect against software malfunction by funding the agent with limited amounts. There is only so much damage the agent can do.

A second challenge to consumer-oriented contract approaches is the claim that companies will ignore consumer-proffered contract terms and that courts will enable them to continue doing so.⁴⁸ This is a non-trivial concern, yet there is hope. Cryptocurrency-fueled smart contracts offer a digital cash-on-the-barrelhead transaction. For a range of transactions, the consumer is protected. Her personal information is safe. If the company does not offer what the consumer seeks, the agent does not act, and the contract is not concluded. This leaves as a risk only those transactions in which a company has made representations to an agent on which the company then reneges. Here there is some hope

47. Clay Shirky, *Transcript—How Social Media Can Make History*, TED (June 2009), http://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history/transcript (last visited Aug. 15, 2014) (noting that, in the context of the social media revolution, online “tools don’t get socially interesting until they get technologically boring”) (on file with the Washington and Lee Law Review).

48. See *supra* notes 31–38 and accompanying text (demonstrating how this concern arises under the current legal regime of the battle of the forms).

that a court will apply more traditional, dickered, black letter law to enforce the consumer-proffered contract. There is at least some chance of convincing courts that the seller has accepted the buyer's offer, rather than the other way around.

A third challenge comes from theorists who are concerned about minimizing overall transaction costs for the online economy. These theorists see contract standardization as positive because it reduces information costs, and they see companies as a better source for standardization than consumers.⁴⁹ The concern is that if companies are forced to respond to thousands of one-off unique consumer contractual proposals, they will not be able to create the economies of contractual scale that are necessary to reduce costs.⁵⁰

These theorists are half right. Standardization is important to reduce transaction costs. Indeed, standardization is necessary in order to create contracts that are sufficiently standardized to become machine-readable. Where the information-cost theorists go wrong is in assuming that companies are a better source of standardized deals than are consumers. Companies create prolix and confusing online contracts. Consumers merely want the standard deal, with no complex reservations. A pro-consumer standardized contract is simple: all remedies and rights are reserved. A corporate-drafted contract, even for a relatively straightforward consumer purchase, can run into tens of pages. Consumers minimize complexity. Companies minimize their legal risk, even (perhaps especially) when doing so increases complexity.

Companies may of course refuse to do business with consumer-originated automated agents, just as companies may refuse to accept crypto-currencies. Yet this is very unlikely. Consider that companies already retool—indeed, optimize—their websites at significant cost to accommodate automated agents, such as

49. See Lucian A. Bebchuk & Richard A. Posner, *One-Sided Contracts in Competitive Consumer Markets*, 104 MICH. L. REV. 827, 834–35 (2006) (arguing that one-sided, seller-oriented form contracts actually minimize transaction costs because of the seller's inability to determine, *ex ante*, which consumers would abuse the contractual relationship without harsh standardized terms); James Gibson, *Vertical Boilerplate*, 70 WASH. & LEE L. REV. 161, 205 n.114 (2013) (providing a list of authors and authorities in support of this proposition).

50. See Robert A. Hillman & Jeffrey J. Rachlinski, *Standard-Form Contracting in the Electronic Age*, 77 N.Y.U. L. REV. 429, 442 (2002) (arguing “the aggregate decisions of many consumers can pressure businesses into providing an efficient set of contract terms in their standard forms”).

Google's web crawlers. Those robots are consumer agents by extension: they gather information, which is placed at consumers' disposal. To a large extent, the search side of the online purchasing equation has already been automated. What remains is to automate the purchase itself, which is what crypto-currency-backed smart contracts can do.

VI. Conclusion

Currency uses of TPLs are merely the first wave of the technology. The math is out of the bag. While TPLs began by proposing a solution disintermediating online property, that disintermediation is likely to affect other areas of law. One area that has long been ripe for reform is consumer contracting. To date, mass-market contracting has rested on the principle that companies can, through their design of the technological contracting process, exclude expressions of consumer preference, and that courts will tacitly support this effort by excluding consumer terms from the four corners of the electronic contracts courts enforce.

Smart contracts will test the poorly conceived legal foundations of the current mass-market consumer-term-exclusion regime. Crypto-currency-backed autonomous agents can offer to buy items without any need to pass on the consumer's identity or payment information. Such agents can further offer digital cash-on-the-barrelhead contracts. It will be much more difficult for a vendor who has accepted such a deal to then later assert that it is not bound by the contractual terms offered by the agent.

Disintermediation has chain effects. Although the debate surrounding Bitcoin and similar crypto-currencies has almost entirely focused on the effect of such systems on the payments and banking infrastructures, there will be more, and more important, changes that will result from the placing of online financial control back into consumers' hands. Once smart contracts answerable to consumers alone are doing the shopping, vendors will either have to respect consumer-proffered contractual demands, or petition courts to continue to undermine consumer contracting power online. Both will happen, but the former is more likely. Those

companies who choose to challenge, rather than respect, consumer-driven smart contract purchases will simply not get paid.