Nebraska Law Review

Volume 96 | Issue 2 Article 8

2017

Conceptualizing Cryptolaw

Carla L. Reyes
Stetson University College of Law, rreyes@cyber.harvard.edu

Carla L. Reyes*

Conceptualizing Cryptolaw

TABLE OF CONTENTS

* Bruce R. Jacob Visiting Assistant Professor of Law, Stetson University College of Law; Faculty Associate, Berkman Klein Center for Internet & Society at Harvard University. J.D., *magna cum laude*, and LL.M. in International and Comparative Law from Duke University School of Law; M.P.P. from the Duke Terry Sanford School of Public Policy. Prior versions of this Article were presented at the 2016 National Business Law Scholars Conference, the 2016 Junior Scholar Virtual Colloquium, and the Coalition of Automated of Legal Applications (COALA) December 2016 Blockchain Workshop in Nairobi, Kenya. Special thanks to Professors Lou Verelli and Ben Edwards for their thoughtful feedback on earlier versions of this Article.

I. INTRODUCTION

At the COALA[1] Blockchain Workshop held in Sydney, Australia, in December 2015,[2] conference goers walk past a metal flower art installation as they enter the auditorium to attend a panel session at the Powerhouse Museum. The uncurious observer might think the metal flower a mere statue. A closer look, however, reveals the flower represents an autonomous life-form affectionately referred to as a "Plantoid."[3] A Plantoid, not owned by any one benefactor, derives its existence from a specialized form of computer code called a decentralized autonomous organization (DAO).[4] If an onlooker passing by the Plantoid sufficiently appreciates the Plantoid's artistic qualities, the onlooker may send a donation to the Plantoid through the decentralized virtual currency called bitcoin.[5] The onlooker sends the bitcoin directly to a wallet owned by the Plantoid itself. As an expression of gratitude for the funds transfer, the Plantoid performs a dance for the onlooker.[6] Once the Plantoid raises sufficient funds, the Plantoid ad-

1. COALA stands for the Coalition of Automated Legal Applications, which is a multi-stakeholder, international, collaborative research-and-development initiative focused on blockchain technologies, smart contracts, and decentralized applications. For more information, see COALA, http://coala.global [https://perma.unl.edu/NZP5-H9VE].
2. BLOCKCHAIN WORKSHOPS: SYDNEY EDITION, http://sydney.blockchainworkshops.org/index.html [https://perma.unl.edu/CMR8-777H].
3. *I'm a Plantoid: A Blockchain-Based Life Form*, OKHAOS, http://okhaos.com/plantoids [https://perma.unl.edu/8DMB-GU4N].
4. *Id.*
5. *Id.*
6. *Id.*

vertises for, selects, and commissions an artist to create a new Plantoid.[7] In other words, all on its own, the Plantoid's computer code enables it to find ways to reproduce.

The advances in technology that enable art to autonomously own assets and reproduce have the potential to alter myriad traditional structures. Predicting that such changes include autonomously acting machines conducting businesses with other machines, one writer suggests that "[s]oon it's just the law in the way, not the technology anymore."[8] But what if the law was not in the way? What if, instead, the law equally experienced transformation induced by the very same advances in technology that propel the Plantoid to reproduce? Indeed, Sweden's current efforts to transfer its real-property recording system to the blockchain,[9] Cook County, Illinois,' efforts to test a similar system,[10] Delaware's efforts to allow corporations to issue shares on the blockchain,[11] Dubai's plans to issue blockchain-based government documents,[12] the U.S. Department of Health and Human Services' interest in using blockchain systems to manage health data,[13] and the European Union's research into blockchain-based regulation for finan-

7. *Id.*
8. HENNING DIEDRICH, ETHEREUM 67 (2016).
9. Pete Rizzo, *Sweden Tests Blockchain Smart Contracts for Land Registry*, COINDESK (June 16, 2016), http://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry [https://perma.unl.edu/5556-44FD].
10. JOHN MIRKOVIC, COOK CTY. RECORDER OF DEEDS, BLOCKCHAIN PILOT PROGRAM: FINAL REPORT (2017), http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf [https://perma.unl.edu/ZN3D-YUWJ].
11. Pete Rizzo, *Delaware Governor Signs Blockchain Bill into Law*, COINDESK (July 24, 2017), https://www.coindesk.com/delaware-governor-signs-blockchain-legislation-law [https://perma.unl.edu/4CFA-LP4Z].
12. Michael del Castillo, *Dubai Wants All Government Documents on Blockchain by 2020*, COINDESK (Oct. 5, 2016), http://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020 [https://perma.unl.edu/HA2A-DXNG].
13. Joseph Bradley, *U.S. Department of Health Calls for Blockchain Research*, CRYPTOCOINSNEWS (Aug. 7, 2016), https://www.cryptocoinsnews.com/u-s-department-of-health-calls-for-blockchain-white-papers [https://perma.unl.edu/JQ2J-J7B9]. State governments are also interested in applying blockchain-based systems to improve government processes. Illinois issued a Request for Information in December 2016, explaining that one of the three areas of focus of its Illinois Blockchain Initiative includes "exploring specific Blockchain and distributed ledger applications and prototypes for use in Illinois government." CRAIG HOLLOWAY, DEP'T OF INNOVATION & TECH., STATE OF ILLINOIS: REQUEST FOR INFORMATION (RFI): DISTRIBUTED LEDGER AND BLOCKCHAIN APPLICATIONS IN THE PUBLIC SECTOR 3 (2016), https://www2.illinois.gov/sites/doit/Documents/BlockchainInitiative/RFI+Blockchain+and+Distributed+Ledger+Applications+in+the+Public+Sector.pdf [https://perma.unl.edu/7TSR-6BFM]. Illinois stated that its specific areas of interest include: (1) identity, attestation, and ownership registries; (2) compliance and reporting ledgers; (3) benefit and entitlement ledgers; and (4) a group of new products and services including escrow as a service, governmental distributed ledgers, and securing the Internet of Things infrastructure. *Id.* at 5–6.

cial institutions[14] suggest that such legal transplants are already underway.

Current strands of law-and-technology literature suggest that technology can both help regulators more efficiently tailor law to rapidly changing industries[15] and help citizens understand their obligations more clearly.[16] Meanwhile, others argue that applying these advances in technology to the law will only lead to new difficulties.[17] In particular, scholars voice concern over the potential for technology to spread and institutionalize the bias of its developers.[18] Taken together, then, the literature suggests that although technology has the potential to make law more efficient and precise, it also introduces new perils. But what if shifting attention to the Distributed Ledger Technology (DLT) that powers the Plantoid, which has not yet been systematically considered for its impact on lawmaking, could increase efficiency, precision, and clarity, and could do so in a transparent way that would help root out systemic bias? Herein lies the promise of "crypto-legal structures": the law of any subject matter implemented and delivered through smart-contracting, semi-autonomous cryptographic computer code.

This Article reveals the emergence of crypto-legal structures and examines their potential for generating new legal discourse around theories of legal process, lawmaking, adjudication, and academic inquiry. DLT offers an opportunity to construct new legal structures which will give rise to new substantive legal issues and cause shifts in legal culture and legal structures. As these new structures emerge, they will endogenously reorder inquiries into the nature of law generally. This Article aims to conceptualize cryptolaw as a disruptive legal discourse that anticipates the new issues arising from the emerging phenomena of crypto-legal structures.

This Article advances the literature in three primary ways. First, this Article turns the current academic discussion relating to DLT and crypto-currencies on its head. Most of the existing literature focuses

14. DIEDRICH, *supra* note 8, at 19.

15. Wulf A. Kaal & Erik P.M. Vermeulen, *How to Regulate Disruptive Innovation—From Facts to Data*, 57 JURIMETRICS (forthcoming 2017), http://ssrn.com/abstract=2808044 [https://perma.unl.edu/NNG6-UCNQ].

16. Anthony J. Casey & Anthony Niblett, *The Death of Rules and Standards*, 92 IND. L. REV. (forthcoming 2017) (describing the potential for microdirectives to emerge from advances in predictive technology and predicting that microdirectives will eliminate the traditionally dichotomous choice between rules and standards faced by lawmakers).

17. Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 4, 11 (2014) (describing the process by which human biases are embedded into the source code of predictive algorithms and describing the lack of transparency into the formulas as examples of these new difficulties).

18. *Id.* at 13–16.

on how to regulate the technology[19] and its various uses.[20] This Article instead considers whether and to what extent DLT will alter the way we think about law itself. While some scholars have considered whether and how DLT may disrupt specific subject areas,[21] this Article examines DLT's broader implications for lawmaking and regulation. Second, this Article builds on two strands of the law-and-technology literature. Specifically, this Article connects insights from one strand, which looks at the effects of predictive technology on regulation and consumer protection,[22] to the other strand, which looks at how the code that constitutes the basic building blocks of new technology can itself serve as a form of law,[23] and uses those connections to

19. Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016) (proposing a technology-enabled endogenous form of DLT regulation); *see* Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359 (2016) (arguing that cryptocurrencies can be used to create peer-to-peer law that governs DLT, even open-source DLT); Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of *Lex Cryptographia* (Mar. 12, 2015) (unpublished manuscript) http://ssrn.com/abstract=2580664 [https://perma.unl.edu/E39V-QFCG] (proposing self-regulation for DLT and arguing that users will create their own rules to govern transactions).

20. *See, e.g.*, Jerry Brito, Houman Shadab & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144 (2014); Primavera De Filippi, *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*, 3 INTERNET POL'Y REV. 1 (2014); Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015); Even Hewitt, Note, *Bringing Continuity to Cryptocurrency: Commercial Law as a Guide to the Asset Categorization of Bitcoin*, 39 SEATTLE U. L. REV. 619 (2016); Ed Howden, Comment, *The Crypto-Currency Conundrum: Regulating an Uncertain Future*, 29 EMORY INT'L L. REV. 741 (2014); Marcel T. Rosner & Andrew Kang, Note, *Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study*, 114 MICH. L. REV. 649 (2016).

21. *See, e.g.*, Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015) [hereinafter Fairfield, *BitProperty*] (examining the potential for DLT disruption in the area of property law); Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35 (2014) [hereinafter Fairfield, *Bitcoin Bots*] (discussing the possibility of DLT disruption in the area of contract law); Wright & De Filippi, *supra* note 19 (arguing that rules for private-law issues will arise through a form of DLT common law).

22. *See, e.g.*, Benjamin Alaire, Anthony Niblett & Anthony Casey, *Law in the Future*, 66 U. TORONTO L.J. 423 (2016); Benjamin Alaire, *The Path of the Law Towards Legal Singularity*, 66 U. TORONTO L.J. 443 (2016); Anthony J. Casey & Anthony Niblett, *Self-Driving Laws*, 66 U. TORONTO L.J. 429 (2016) [hereinafter Casey & Niblett, *Self-Driving Laws*]; Citron & Pasquale, *supra* note 17; Casey & Niblett, *supra* note 16; Kaal & Vermeulen, *supra* note 15.

23. *See, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE VERSION 2.0 (2d ed. 2006); Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275 (2002); Lawrence Lessig, *Open Code and Open Societies: Values of Internet Governance*, 74 CHI.-KENT L. REV. 1405 (1999); David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace*, 52 STAN. L. REV. 1439 (2000).

reveal the potential power of crypto-legal structures. Third, this Article uses comparative legal methodology to conceptualize the impact of crypto-legal structures on the foundations of the law itself. This Article demonstrates that by treating computer code as a foreign legal system, methodological tools from comparative law enables lawmakers and regulators to predict the broader ramifications of shifting existing legal rules to crypto-legal structures. In doing so, the Article reveals a legal world with more overlap between legal systems, simplified substantive law, new regulatory agents, legal culture heavily influenced by computer software developers, and an evaporating gap between the law-in-action and the law-in-the-books. By connecting the literature on DLT, law and technology, and comparative law, this Article offers a conceptual framework for a new legal discourse and jurisprudence of cryptolaw and argues that cryptolaw will fundamentally change the way law is implemented, updated, experienced by citizens, and adjudicated.

This Article proceeds in five Parts. Part I briefly describes DLT and smart contracts. Part II proposes the conceptual contours of crypto-legal structures, outlines two concrete examples of crypto-legal structures, and addresses the anticipated concern that crypto-legal structures and cryptolaw are just another "law of the horse."[24] Using comparative law as a methodological tool, Part III analyzes cryptolaw's potential to disrupt discourse regarding the fundamental elements of law: substantive law, legal structure, and legal culture. Part IV examines the feasibility of adopting crypto-legal structures and explores the implications and broader consequences of cryptolaw's emergence. A final Part concludes.

II. A DISTRIBUTED LEDGER TECHNOLOGY PRIMER

This Article begins by offering a brief introductory explanation of "distributed ledger technology" (DLT). This Article uses the term distributed ledger technology, or DLT, to refer broadly to distributed network technology that (1) enables users to upload programs and to leave the programs to self-execute; (2) maintains a public, tamper-resistant record (ledger) of the current and past states of every program; (3) is distributed; (4) uses public key cryptography for authentication; and (5) uses a consensus mechanism to ensure that the network maintains the technology.[25] This Article adopts this definition because it is broad enough to encompass various forms of DLT, including the

24. For a full explanation of the origin of and debate surrounding the phrase "the law of the horse," see *infra* notes 93, 150–155 and accompanying text.

25. *See* Reyes, *supra* note 19, at 191 n.1 (citing Vitalik Buterin, *Visions, Part 1: The Value of Blackchain Technology*, ETHEREUM BLOG (Apr. 13, 2015), https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology [https://perma.unl.edu/4EJG-KJKA]).

Bitcoin blockchain, the Ripple Protocol, Ethereum, and others.[26] Although subtle, an important point is that the term DLT, as used in this Article, is broad enough to encompass both proprietary (permissioned) DLT and open-source (permissionless) DLT.[27] With these boundaries of the term DLT in mind, section II.A. first offers a brief introduction to the technology and its variants. Section II.B. then introduces the concept of smart contracts, which are enabled by DLT and will form the building blocks of crypto-legal structures.

A. Distributed Ledger Technology: Bitcoin's Blockchain, Ethereum, and Beyond

Distributed ledger technology (DLT) refers to computer software that is distributed, runs on peer-to-peer networks,[28] and offers a transparent,[29] verifiable, tamper-resistant transaction-management

26. For further explanation see *infra* note 29. Note, furthermore, that this Article's definition of DLT is not intended to limit DLT protocols to database functions. DIEDRICH, *supra* note 8, at 88 ("So if you can't help but have to think of a blockchain as a database, then this can be thought of as database triggers firing off after a state change. That's nothing new, obviously. But again, the innovation is that this happens simultaneously on all nodes of the network and can't be stopped. Plus, that anything going in must be digitally signed by an account holder. Which is nothing like a database. It's a blockchain.").

27. This stands in contrast to other work in this space, which has focused heavily on the Bitcoin blockchain, where the DLT at issue is open-source. *See, e.g.*, Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 843 (2015) (defining the Bitcoin Blockchain as "peer-to-peer open-source software that operates to create and maintain a distributed public ledger" (footnotes omitted)).

28. Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. L. REV. ONLINE 1485, 1488 (2014) ("Bitcoin is a peer-to-peer software system, which means, practically speaking, that the entire system is made up of versions of the software that end-users download and run on their personal computers. There is no Bitcoin server or Bitcoin company that directly manages the system." (emphasis omitted)).

29. Note that this Article uses "transparent" instead of "public" to define the nature of the ledger. This intentional choice keeps the definition of DLT broad enough to encompass both permissionless and permissioned ledgers. The open-source, or permissionless, DLT are generally public ledgers, open for anyone to inspect. Walch, *supra*, note 27, at 840 & n.15. Permissioned DLT, on the other hand, are developed and used on a proprietary basis and are often not public. *Id.* Nevertheless, in such permissioned DLT, it is possible to give keys to certain outsiders (e.g., regulators) for the purpose of inspecting the ledger. As such, permissioned DLT remains transparent, even if it is not public in the same way as permissionless DLT. I am aware of objections to the idea of "permissioned" DLT insofar as the concept necessarily means the permissioned ledger is not as decentralized as the permissionless originals. I do not engage that debate here and do not intend to do so. Because permissionless DLT exists and is in use, this Article takes the position that any legal discussion of DLT must consider both forms of DLT. Otherwise, whatever paradigm put forth risks missing important implications for the law. To that end, my use of the term "distributed ledger technology" as opposed to "decentralized ledger technology" is intentional. I suggest that permis-

system maintained through a consensus mechanism rather than by a trusted third-party intermediary[30] that guarantees execution.[31] DLT is essentially "a chronological database of transactions recorded by a network of computers"[32] that "has rules and built-in security . . . and . . . maintains internal integrity and its own history."[33] In other words, DLT "provide[s] a distributed yet provably accurate record . . . [such that] everyone can maintain a copy of a dynamically-updated ledger, but all those copies remain the same, even without a central administrator or master version."[34] By "combining peer-to-peer networks, cryptographic algorithms, distributed data storage, and a [sic] decentralized consensus mechanisms,"[35] DLT offers a mechanism, maintained by a distributed network over which no one person or entity maintains control, for managing transactions and ensuring the transactions are executed.[36] One of the most well-known examples of DLT is the Bitcoin[37] blockchain.[38] The Bitcoin blockchain encrypts transactions and breaks them into smaller sets of aggregated transactions called "blocks."[39] A block groups transactions, marks

---

sioned and permissionless ledgers are both distributed, but only permissionless ledgers have the potential to be truly decentralized, recognizing, of course, that at present, certain purported decentralized permissionless ledgers are not very decentralized at all.

30. Bayern, *supra* note 28, at 260 (describing this feature of DLTs as a "decision to avoid what network theorists call a trusted third party—that is, an authority, above reproach, that can inform others of the canonical state of the system" (emphasis omitted)).
31. DIEDRICH, *supra* note 8, at 5.
32. Wright & De Filippi, *supra* note 19, at 6 (citation omitted); *see also* PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 124 (2015) ("The blockchain doesn't live on a single computer or server but . . . is shared around that community of computer owners, or nodes." (emphasis omitted)).
33. DTCC, EMBRACING DISRUPTION: TAPPING THE POTENTIAL OF DISTRIBUTED LEDGERS TO IMPROVE THE POST-TRADE LANDSCAPE 7 (2016), http://www.dtcc.com/news/2016/january/25/blockchain-white-paper.
34. Kevin Werbach, Trustless Trust 2 (Aug. 8, 2016) (unpublished manuscript) (footnote omitted), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757380.
35. Wright & De Filippi, *supra* note 19, at 4–5.
36. Fairfield, *Bitcoin Bots*, *supra* note 21, at 36.
37. In technology circles, the Bitcoin software, protocol, and network are referenced using the upper case "Bitcoin" while the lower case "bitcoin" refers to individual units of account. Walch, *supra* note 27, at 846 & n.41 (citing *Vocabulary*, BITCOIN, https://bitcoin.org/en/vocabulary [https://perma.unl.edu/3R8G-STQT]).
38. J. ANTHONY MALONE, BITCOIN AND OTHER VIRTUAL CURRENCIES FOR THE 21ST CENTURY 35 (2014); Paul H. Farmer, Jr., Note & Comment, *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85, 88–89 (2014) ("The Bitcoin peer-to-peer network that allows for miners to generate Bitcoins also serves as a public ledger for all Bitcoin transactions. A timestamp server records the time of creation of each Bitcoin and any other Bitcoin transaction within the network. The full record of transactions is called a block chain, a sequence of records composing a virtual ledger." (footnotes omitted)).
39. MALONE, *supra* note 38, at 35.

them with a timestamp, and connects them to the previous block in the chain of transactions, leading to the name blockchain.[40] New blocks of transactions are only added to the chain after they have been verified.[41]

Although the precise mechanics of building and maintaining the ledger vary, most DLTs use two techniques to confirm and secure transactions. First, most DLTs use cryptographic public–private key pairs to secure and authorize an entry in a ledger.[42] The public key acts as a publicly identifiable address to which transactions may be directed (like a bank account or email address), while the private key allows the person or entity to whom the public key corresponds to originate transactions (the way a bank-account PIN authorizes its holder to originate funds transfers or an email password allows its holder to originate messages).[43] This cryptographic key pair enables secure peer-to-peer transactions by ensuring that only the holder of the private key can initiate the transaction.[44] For example, when an onlooker appreciates the Plantoid enough to give the Plantoid bitcoin, the onlooker uses her private key to initiate the funds transfer to the Plantoid's public key (its "bitcoin wallet address"). Once received by the Plantoid, the onlooker can trust that only the Plantoid can spend the bitcoin because a new transaction with that bitcoin can only be

40. ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN xix, 160 (2015); *see also* Fairfield, *BitProperty*, *supra* note 21, at 814 ("The Bitcoin protocol creates a ledger out of a series of groups of transactions, termed simply 'blocks,' which as a whole form a log of all transfers, termed the 'block chain.' The block chain is not maintained by any single entity, but instead relies on a mathematically innovative consensus model." (footnotes omitted)).

41. Abramowicz, *supra* note 19, at 371 ("The block chain includes only transactions that are verified as legitimate." (footnotes omitted)).

42. Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 117 (2012).

43. Reyes, *supra* note 19, at 200. For example, when a user of the Bitcoin Blockchain sends bitcoin to another Bitcoin Blockchain user, the bitcoin holder uses his or her private key to authorize the transfer of bitcoin to the public address representing the recipient's wallet. Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441, 446 (2014); *see also* Bayern, *supra* note 28, at 260 ("Just as someone without my password could not log into my credit union account, someone without my private Bitcoin keys could not spend my bitcoins.").

44. Abramowicz, *supra* note 19, at 372 ("A mathematical technique can be used to quickly generate two keys of a specific length (say, 256 bits). One of the keys can be used to scramble a communication, and the other key can then unscramble it. This method can be used to authenticate documents. For example, a 'hash function' can create a short code from a document, essentially a fingerprint. The authenticator then scrambles (encrypts) this code using the private key. The public key can be used to decrypt it, producing the original hash. Thus, anyone who knows the relevant algorithms and the public key can conclude, with near certainty, that someone who knew the private key corresponding to the public key must have performed the encryption." (footnotes omitted)).

initiated by the Plantoid's use of the unique private key corresponding to its public key.

Most DLTs also use some form of incentivized network consensus to verify the accuracy of transactions pushed to the ledger.[45] "Consensus means that participants in a network have confidence that what they see on their ledgers is accurate and consistent."[46] In the case of the Bitcoin blockchain, the consensus method is referred to as mining, a process by which nodes[47] vote on the correct state of the ledger such that "[e]very full node sees every transaction, and there is only one consensus ledger mirrored across every machine on the network."[48] To prevent cheating and ensure the validity of the ledger, the Bitcoin blockchain uses a proof-of-work[49] consensus process in which Bitcoin blockchain nodes solve complex mathematical problems to validate each block.[50] Solving the mathematical problems, which are "cryptographic puzzles involving one-way functions known as hashes," requires intense and expensive computing power.[51] The difficulty and expense of validating a block deters cheating and fraudulent verification.[52]

45. SIGRID SEIBOLD & GEORGE SAMMAN, CONSENSUS: IMMUTABLE AGREEMENT FOR THE INTERNET OF VALUE 2 (2016), https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf [https://perma.unl.edu/P7GH-DQRF]; *see also* Abramowicz, *supra* note 19, at 373 (describing the Bitcoin Blockchain solution for verifying transactions by consensus).

46. Werbach, *supra* note 34, at 25.

47. DIEDRICH, *supra* note 8, at 9 n.4 ("A 'node' is usually one computer, no matter the size. But more strictly, it's one instance of a client program running. This could be multiple times on one and the same computer. In which case, that computer would be said to host multiple nodes.").

48. Werbach, *supra* note 34, at 26.

49. A proof-of-work consensus model "require[s] the client requesting the service prove that some work has been done" in order to process the request. PEDRO FRANCO, UNDERSTANDING BITCOIN: CRYPTOGRAPHY, ENGINEERING, AND ECONOMICS 102 (2015).

50. ANTONOPOULOS, *supra* note 40, at xx (describing a miner as "[a] network node that finds valid proof of work for new blocks, by repeated hashing"); FRANCO, *supra* note 49, at 103 ("To secure the blockchain—the distributed transaction database—Bitcoin requires proof-of-work to be performed on blocks of transactions following the Solution-Verification protocol."); MALONE, *supra* note 38, at 36.

51. Werbach, *supra* note 34, at 27.

52. *Id.*; *see also* Bayern, *supra* note 28, at 261–62 ("The precise mechanism by which Bitcoin produces this authoritative sequence is complex, but in short, and loosely speaking, it allows participants to add new financial records to the authoritative sequence by demonstrating that they have expended computing power on an otherwise unimportant, repetitive task. This process, known as Bitcoin mining, confers the right to add a record to the sequence (and also, not incidentally, it is rewarded by the creation of new bitcoins, partly as an incentive to participate in the network and partly as a way to manage the initial distribution of bitcoins). In the event of a dispute among different candidate sequences of transactions, the

Other DLT consensus models include "unique node list" consensus[53] and proof-of-stake consensus,[54] among several others.[55] "The basic premise is that all nodes control each other all the time and they can do that because they know exactly what every other node *should* hold as truth at any given time. If all nodes agree, this is called *consensus*."[56] In other words, "[e]very node in a blockchain stores and computes the *same* data."[57] In Ethereum, for example, "every transaction that was ever made, every contract that was ever invoked, is relived by [each node]."[58] This allows each node to ensure that "the data it is receiving is consistent and double checks the global state of the Ethereum network."[59] Ultimately, whatever specific form used, the consensus mechanism and cryptographic signatures replace the tradi-

---

one that is eventually backed by the most computing power wins." (footnotes omitted)).

53. *See* DAVID SCHWARTZ, NOAH YOUNGS & ARTHUR BRITTO, THE RIPPLE PROTOCOL CONSENSUS ALGORITHM 3 (2014), https://ripple.com/files/ripple_consensus_whitepaper.pdf [https://perma.unl.edu/7XMM-7HNS]; Dave Cohen, David Schwartz & Arthur Britto, *The XRP Ledger Consensus Process*, RIPPLE, https://ripple.com/build/ripple-ledger-consensus-process [https://perma.unl.edu/HDH7-CYWE]. In the Ripple Protocol, the candidate set of transactions is validated and becomes part of the permanent, authoritative ledger once the votes from the server nodes reaches eighty percent. Adrian Blundell-Wignall, *The Bitcoin Question: Currency Versus Trust-Less Transfer Technology* 15 (OECD Working Papers on Fin., Ins. & Private Pensions, Paper No. 37, 2014), http://www.oecd.org/daf/fin/financial-markets/The-Bitcoin-Question-2014.pdf [https://perma.unl.edu/LZ7M-EGHV]. At least one commentator has referred to this approach as a "Byzantine agreement system"; however, the creators of the Ripple Protocol do not themselves adopt that terminology. *See generally* DAVID MAZIÈRES, THE STELLAR CONSENSUS PROTOCOL: A FEDERATED MODEL FOR INTERNET-LEVEL CONSENSUS (2016), https://www.stellar.org/papers/stellar-consensus-protocol.pdf [https://perma.unl.edu/7P6C-NQLY].

54. Wright & De Filippi, *supra* note 19, at 7 n.30; *see also* Nicolas Houy, *It Will Cost You Nothing to "Kill" a Proof-of-Stake Crypto-Currency*, 34 ECON. BULL. 1038, 1040 (2014) (describing proof of stake as a consensus mechanism in which "the expected reward for inserting transactions in the blockchain does not depend on the computational power of miners but on the amount of crypto-currency they already own").

55. For example, the Stellar Consensus Protocol uses an approach similar to that of Ripple, which it refers to as a "Federated Byzantine Agreement" consensus model. MAZIÈRES, *supra* note 53. See also the discussion in IDDO BENTOV ET AL., PROOF OF ACTIVITY: EXTENDING BITCOIN'S PROOF OF WORK VIA PROOF OF STAKE (2014), http://eprint.iacr.org/2014/452.pdf [https://perma.unl.edu/4JFL-UMGP] (proposing a new proof-of-activity model by combining a proof-of-work component with a proof-of-stake-type system).

56. DIEDRICH, *supra* note 8, at 20.

57. *Id.* at 33.

58. *Id.*

59. *Id.* (emphasis omitted). Note that "state" refers to "all or part of the data that a program deals with." *Id.* Computer code that remembers things, then, is "stateful" computer code. DLT in general, and Ethereum in particular, is for stateful applications.

tional third-party mediator as the entity maintaining the ledger, and instead the system offers a peer-to-peer basis for trust, accountability, and transparency.[60]

Richard Gendal Brown, the developer spearheading R3's Corda™ distributed ledger for financial services, explains the foundation for DLT's peer-to-peer basis for trust another way. Brown views DLT as offering a bundle of five services which include: (1) consensus, the capacity to "create a world where parties to a shared fact know that the fact they see is the same as the fact that other stakeholders see . . . across the Internet between mutually untrusting parties";[61] (2) validity, the capacity "to know whether a given proposed update to the system is valid";[62] (3) uniqueness, the capacity, in the face of conflicting valid updates to the system, "to know which, if either, of those updates we should select as the one we all agree on";[63] (4) immutability,[64] the feature of DLT whereby "nobody else [in the DLT system]

60. Sloane Brakeville & Bhargav Perepa, *Blockchain Basics: Introduction to Distributed Ledgers*, IBM (May 9, 2016), http://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html [https://perma.unl.edu/9LUW-AR5E]. For example, in Ethereum, when you take the Ethereum consensus mechanism and add the fact that "every single change to the global world state of the Ethereum network has been signed off by the person owning the sender account of the transaction effecting the change" with the result being an outcome of the world state that is indisputable and trustworthy. DIEDRICH, *supra* note 8, at 34–35.

61. Richard Gendal Brown, *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services*, R3 POV (Apr. 5, 2016) (emphasis omitted), https://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services [https://perma.unl.edu/L3EY-K6GN].

62. *Id.*

63. *Id.*

64. As a note on terminology, when someone remarks that DLT is "permanent," or "immutable," they are referring to the technology's ability to track the complete history and the current state of the protocol. This terminology is, however, very simplistic for the complexity of the computer science and mathematical concepts it tries to convey. With regard to the history of transactions in DLT,

> All blockchains have a notion of a history—the set of all previous transactions and blocks and the order in which they took place—and the STATE—'currently relevant' data that determines whether or not a given transaction is valid and what the state after processing a transaction will be. Blockchain protocols also have a notion of A STATE TRANSITION RULE: given what the state was before, and given a particular transaction, (i) is the transaction valid, and (ii) what will the state be after the transaction?

VITALIK BUTERIN, ETHEREUM: PLATFORM REVIEW (2015), https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57506f387da24ff6bdecb3c1/1464889147417/Ethereum_Paper.pdf [https://perma.unl.edu/2MFU-EFD6]. This understanding of transaction history is not always the same understanding lawyers have when they hear or use the terms permanent or immutable, even in reference to DLT. Where appropriate, I use the term "temper resistant" to more accurately reflect to non-computer-scientist readers the use of the term immutable (or permanent) in this context.

will accept a transaction from me if it tries to build on a modified version of some data that has already been accepted by other stakeholders";[65] and (5) authentication, the feature of DLT whereby "every action in the system is almost always associated with a private key; there is no concept of a 'master key' or 'administrator password' that gives God-like powers."[66] Brown considers these five services capable of unbundling and repackaging to serve specific design purposes.[67] Therefore, DLT represents general-purpose technology that can be used to solve any problem to which it is well suited.

B. A Brief Introduction to Smart Contracts

DLTs are also robust enough to allow software developers to layer complex relationships into the computational material of the underlying protocol. In 1994, Nick Szabo first conceptualized such coded relationships as "smart contracts,"[68] which he defined as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[69] Although this term is now frequently used when considering whether natural-language contracts can be adequately translated into computer code or when referring to computer programs that themselves represent a legally binding contract, Szabo's original conception was broad enough that while some smart contracts may fulfill the legal requirements of the word "contract,"[70] some may not.[71] At base, and in line with Szabo's original

65. Brown, *supra* note 61 (emphasis omitted).
66. *Id.*
67. *Id.*
68. S. Asharaf & S. Adarsh, Decentralized Computing Using Blockchain Technologies and Smart Contracts 45 (2017) ("The concept of smart contracts was first formally coined by Nick Szabo in 1994.").
69. Nick Szabo, Smart Contracts: Building Blocks for Digital Markets (1996), http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [https://perma.unl.edu/AX4L-CPC5]; Nick Szabo, *Formalizing and Securing Relationships on the Public Networks*, First Monday (Sept. 1, 1997) [hereinafter Szabo, *Formalizing and Securing Relationships*], http://firstmonday.org/ojs/index.php/fm/article/view/548/469 [https://perma.unl.edu/V6JY-T7RE].
70. *See* Norton Rose Fulbright, Can Smart Contracts Be Legally Binding Contracts? (2016), http://www.nortonrosefulbright.com/files/norton-rose-fulbright—r3-smart-contracts-white-paper-key-findings-nov-2016-144554.pdf [https://perma.unl.edu/963U-UX5A]; Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 Duke L.J. (forthcoming).
71. William Mougayar, The Business Blockchain: Promise, Practice and Application of the Next Internet Technology 42 (2016) ("Smart contracts are not the same as a contractual agreement. If we stick to Nick Szabo's original idea, smart contracts help make the breach of an agreement expensive because they control a real-world valuable property via 'digital means.' So, a smart contract can enforce a functional implementation of a particular requirement, and can show proof that certain conditions were met or not met.").

idea, a smart contract is thus "a computer protocol—an algorithm—that can self-execute, self-enforce, self-verify, and self-constrain the performance" of its instructions.[72] So conceived, the Bitcoin blockchain is itself a limited form of a smart contract.[73] Similarly, the computer code that causes the Plantoid to dance upon receipt of bitcoin is a smart contract.

More complex smart contracts can be created by embedding additional code into the underlying protocol;[74] however, the level of complexity achievable may be determined by the underlying protocol used. For example, Ethereum is a DLT specifically designed to enhance developers' ability to layer complex transaction protocols on top of the base ledger[75] and is thought to thereby enable more complex smart-contract programming.[76] One writer explains that Ethereum goes beyond the Bitcoin blockchain "and allows you to program the future, to

72. MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 16 (2015) ("[A] smart contract is both defined by the code and executed (or enforced) by the code, automatically without discretion."); TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY, AND TRUSTLESS ASSET MANAGEMENT 16 (2014).

73. *See, e.g.*, Werbach, *supra* note 34, at 30 ("Distributed ledgers are active, not passive. In other words, they do not simply record information passed to them. They are part of a consensus system, so they must ensure that recorded transactions are actually completed to match the consensus. For Bitcoin, that means the system self-enforces financial transfers. I can't initiate a transaction promising to send you Bitcoin and then renege; the synchronization that reconciles and completes the transfer is part of the process. This mechanism is known as a smart contract. Both the specification of rights and obligations, and the execution of that contractual agreement, occur through the platform." (footnotes omitted)).

74. MOUGAYAR, *supra* note 71, at 43 ("Smart contracts are not the same as blockchain applications. Smart contracts are usually part of a decentralized (blockchain) application."); SWAN, *supra* note 72, at 16 ("In the blockchain context, contracts or smart contracts mean blockchain transactions that go beyond simple buy/sell currency transactions, and may have more extensive instructions embedded into them."); Werbach, *supra* note 34, at 30–31 ("Adding richer programming capabilities to blockchain transactions adds security risks and various other complexities. On the other hand, a smart contract engine on the blockchain creates enticing possibilities. In technical terms, smart contracts are essentially autonomous software agents. With smart contracts, a distributed ledger becomes functionally a distributed computer." (footnotes omitted)).

75. MOUGAYAR, *supra* note 71, at 43 (noting that Ethereum uses a specific smart-contract language (Solidity), enabling coders to write complex processes in a short span of code); Werbach, *supra* note 34, at 31 ("Newer blockchain platforms remove Bitcoin's limitations on smart contracts. The most prominent is Ethereum, which launched in 2015. Ethereum offers a Turing-complete programming language, meaning that in theory, any application that runs on a conventional computer can be executed on the distributed computer of its consensus network. Ethereum is designed as a complete smart contract platform, including development tools and a browser." (footnotes omitted)).

76. DIEDRICH, *supra* note 8, at 39 ("Ethereum has its focus on smart contracts instead of being exclusively a digital currency. And as part of that, Ethereum transactions can be way more sophisticated than Bitcoin's: full fledged, high language

implement rules governing the array of possibilities that fan out from the present."[77]

The potential uses for smart contracts are limited only by the coders that develop them. Although smart contracts "are ideal for interacting with real world assets, smart property, Internet of Things (IoT), and financial services instruments," they need not be limited in application to the movement of monetary value.[78] Instead, smart contracts "apply to almost anything that changes its state over time, and could have a value attached to it."[79]

The key elements that make smart contracts both unique and powerful lie in their autonomous, self-sufficient, distributed nature. After launching a smart contract, the contract runs autonomously in that the developer does not need to actively maintain, monitor, or even be in contact with it.[80] The operating contract is self-sufficient insofar as it may be programmed to "marshal resources—that is, raising funds by providing service or issuing equity, and spending them on needed resources, such as processing power or storage."[81] Finally, the smart contract is distributed in that it exists as software distributed and operated across a variety of network nodes.[82] Further, each smart contract "will be imbued with some modest form of 'intelligence', statistical algorithms and optimizations."[83]

These advanced qualities make smart contracts a technology tool of general application. Current uses include the securities-trading platform developed and launched by Overstock.com Inc.—the t0 platform.[84] Specifically, "Overstock.com Inc. . . . has issued bonds on the bitcoin blockchain, becoming the first company to offer a crypto-security, and has gained regulatory approval to do the same with equity."[85] Other examples include decentralized file storage[86] and notary ser-

---

programs, some many thousand lines long, which can call each other, almost ad infinitum.").

77. *Id.* at 22 (emphasis omitted).
78. MOUGAYAR, *supra* note 71, at 43.
79. *Id*.
80. SWAN, *supra* note 72, at 16.
81. *Id.* This autonomy and self-sufficiency is aptly demonstrated in current uses of smart contracts. Take, for example, the Plantoid project described in the opening paragraph of this Article. *See supra* notes 1–7 and accompanying text. For more information, see *I'm a Plantoid: A Blockchain-Based Life Form*, *supra* note 3.
82. SWAN, *supra* note 72, at 16.
83. DIEDRICH, *supra* note 8, at 83.
84. David Floyd, *Overstock's t0: Reconciling Fiat Currency and the Bitcoin Blockchain*, NASDAQ (Dec. 16, 2015), http://www.nasdaq.com/article/overstocks-t0-reconciling-fiat-currency-and-the-bitcoin-blockchain-cm555617 [https://perma.unl.edu/H52Q-Q6NT].
85. *Id.*
86. SHAWN WILKINSON, STORJ: A PEER-TO-PEER CLOUD STORAGE NETWORK 2 (2014), https://storj.io/storj2014.pdf [https://perma.unl.edu/LZ3U-5CBY] (outlining a pro-

vices,[87] among others.[88] To date, the law's main concern around smart contracts focuses on determining whether and how the disruptive applications using smart contracts should be regulated. The law and those that develop it, academics and policymakers alike, should prepare for a time when smart contracts and DLT disrupt the law itself. We should prepare for a jurisprudence of cryptolaw: a discussion about law that anticipates new issues emerging as a result of using DLT and smart contracts in regulation, enforcement, and adjudication.

III. DEFINING CRYPTOLAW

Vague references to an emerging law of DLT appear occasionally.[89] When pressed to describe what makes the legal issues facing DLT different from other law-and-technology considerations, many arguments harken back to the 1990s debate about regulation and the Internet. Others point to what arguably represent cryptolaw's precursors.[90] The cryptolaw conceptualized in this Article is not a discussion of whether or how to regulate DLT[91] nor is it a discussion of how new technology can be used to comply with current law.[92] Instead, this Part conceptualizes cryptolaw as the new jurisprudence that will emerge as a result of implementing and delivering the law of any subject matter through smart-contracting, semi-autonomous, intelligently developing cryptographic computer code. This Part argues that a variety of laws and legal structures will benefit from the autonomous, self-executing, transparent nature of DLT. By building such laws into computer-coded legal structures (which this Article calls "crypto-legal structures"), lawmakers will be able to emphasize the specific features of DLT most useful to the legal and social problem at hand. As such crypto-legal structures interact with each other and with those gov-

posal for a "decentralized cloud storage platform that implements end-to-end encryption on a decentralized and open network").

87. Luke Parker, *Bitnation Starts Offering Blockchain Public Notary Service to Estonian e-Residents*, BRAVE NEW COIN (Dec. 1, 2015), http://bravenewcoin.com/news/bitnation-starts-offering-blockchain-public-notary-service-to-estonian-e-residents [https://perma.unl.edu/KY8S-M8NZ].

88. For a more complete discussion of potential and developing use cases, see DIEDRICH, *supra* note 8, at 58–69; *see also* SMART CONTRACTS ALLIANCE & DELOITTE, SMART CONTRACTS: 12 USE CASES FOR BUSINESS & BEYOND (2016), http://www.digitalchamber.org/smartcontracts.html (describing two cases for using smart contracts).

89. *See infra* note 145 and accompanying text.

90. Werbach, *supra* note 34, at 73–77 (describing a process for using DLT to supplement existing laws).

91. *See*, *e.g.*, Brito et al., *supra* note 20; De Filippi, *supra* note 20; Reyes, *supra* note 19; Tu & Meredith, *supra* note 20; Hewitt, *supra* note 20; Howden, *supra* note 20; Rosner & Kang, *supra* note 20.

92. Werbach, *supra* note 34, at 73–78.

erned by the law, a broader set of new legal principles and issues will emerge as cryptolaw. Sections III.A. and III.B. help concretize this new system by exploring cryptolaw in the context of two examples. Finally, section III.C. concludes by arguing that, taken together, crypto-legal structures and the related new legal constructs in cryptolaw thereby constitute a new theory or philosophy of law, thus demonstrating that cryptolaw is more than another "law of the horse."[93]

A. Distributed Ledger Technology Will Lead to Cryptolaw

The use of DLT and its smart-contracting capacity by governments will lead to the emergence of cryptolaw: a new legal discourse anticipating the issues arising from implementing, enforcing, and adjudicating law through smart-contracting, semi-autonomous cryptographic computer code. I advanced an initial framework for implementing and delivering law through cryptographic, smart-contracting computer code in a prior article,[94] where I argued that regulation implemented and delivered through code solves the riddle of how to regulate DLT and its many use cases without stifling innovation. This Article expands on that base by arguing that the endogenous theory previously proposed can be applied to any substantive area of law to create crypto-legal structures. The Article goes on to explore the doctrinal and jurisprudential ramifications of crypto-legal structures, offering a conceptual framework for cryptolaw—a new area of legal discourse.

Conceptualizing cryptolaw requires envisioning a world in which law is created first through legislation or regulation written in words and then implemented through cryptographic, smart-contracting computer code.[95] The creation and implementation of any individual element of cryptolaw (which this Article refers to as a crypto-legal structure) may occur in a variety of ways, each varying in its degree of endogenous origins, jurisdictional application, and the degree to which its implementation relies entirely upon DLT, or on a mix of DLT and existing legal structures. The ability to rapidly tailor the method and locus of creating crypto-legal structures to the need of the legal or policy problem represents one of its core beneficially disruptive elements. Furthermore, recognizing that DLT offers a diverse array of architecture to choose from addresses a frequent objection that certain indus-

93. The "law of the horse" is a term Frank Easterbrook coined in reference to the law of cyberspace, quipping that the law of cyberspace is merely a specialized endeavor to which general legal rules could be applied as problems arose on a case-by-case basis, rather than a separate area of law. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–208. For a more detailed discussion of the "law of the horse," see *infra* notes 150–55 and accompanying text.

94. Reyes, *supra* note 19.

95. *Id.* at 228.

try actors, governments, and academics seek to apply DLT in inappropriate contexts simply because DLT is the hot technology innovation of the day.

Specifically, some argue that the recent hype around DLT is leading to its use in areas where DLT is not necessary[96] and that doing so can lead to unnecessary design flaws in key structures.[97] Under this line of thinking, new technology, including DLT, should only be applied to circumstances in which the technology offers the right solution to a specific problem.[98] Under what circumstances, then, will it be appropriate to apply DLT to the law? In many areas, law adapts slowly to current realities and new technologies, stifling innovation.[99] In other areas, the law requires a clear record or evidence that in practice is very difficult to obtain in a verifiable way.[100] In yet other areas, regulatory complexity or uncertainty paralyzes individuals or business entities and prevents them from acting.[101] In conceptualizing the broader ramifications of crypto-legal structures (some of which are being created by governments right now)[102] on the law, this Article asks whether and under what circumstances DLT is the appropriate mechanism for addressing these problems of law lag, inefficiency, usability, and transparency.

Many coders, such as R3's Richard Gendal Brown, view DLT as a bundle of five services (consensus, validity, uniqueness, immutability, and authentication)[103] that can be selected, like items on a menu, in whatever combination is needed to address a problem.[104] Taken together, these five services of DLT lead to "the emergence of platforms, shared across the Internet between mutually distrusting actors, that

96. DIEDRICH, *supra* note 8, at 49–50 (demonstrating that many current proposals for blockchain-based applications are really database, cloud-service, or cryptography-based applications instead).

97. Brown, *supra* note 61.

98. *Id.*

99. Jeremy Pitt & Ada Diaconescu, *The Algorithmic Governance of Common-Pool Resources*, *in* FROM BITCOIN TO BURNING MAN AND BEYOND: THE QUEST FOR IDENTITY AND AUTONOMY IN A DIGITAL SOCIETY 130, 137–38 (John H. Clippinger & David Bollier eds., 2014).

100. For example, consider the U.C.C. Article 9 Filing System. *See* LYNN M. LOPUCKI, ELIZABETH WARREN & ROBERT LAWLESS, SECURED TRANSACTIONS: A SYSTEMS APPROACH 281–82 (8th ed. 2016) ("[F]iling systems are highly imprecise and difficult and expensive to use. Filing is relatively easy. But searching is relatively difficult . . . .").

101. For example, consider the application of federal and state money-transmission laws to the financial-technology ("FinTech") industry. The laws applicable to the money-transmission context exist at both the state and federal levels, and violations are punishable by criminal penalties, including prison. Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383 (2017).

102. *See supra* notes 9–14 and accompanying text.

103. For a full discussion of each service, see *supra* text accompanying notes 61–66.

104. Brown, *supra* note 61.

allow them to reach consensus about the existence and evolution of facts shared between them."[105] To determine, then, whether a particular area of the law will benefit from the application of DLT, we must consider whether the root of the identified problem of law lag, inefficiency, usability, or transparency relates to difficulty in reaching a consensus about the existence and evolution of shared facts. If so, that area of the law is ripe for crypto-legal-structure development. In such circumstances, the goal is to choose from the menu of DLT services to implement the law through smart-contracting distributed computer code in a way that addresses the identified problem.[106] When conceived of in this light, crypto-legal structures represent a general-purpose form of implementing and adjudicating law. Crypto-legal structures are not limited by the context in which they are applied because the DLT underlying the structures can be unbundled and repackaged to address any specific context.

To concretize this idea, consider the implications of a shared record of immutable, verifiable, unique, authenticated facts for the Uniform Commercial Code's Article 9 filing system. Article 9 of the Uniform Commercial Code (U.C.C.) governs security interests in personal property.[107] Protection of a secured creditor's interest in the collateral used to secure the loan it made vis-à-vis the interests of other secured creditors depends, in part, upon the ability of a secured creditor to communicate the existence of its interest to other potential creditors.[108] To this end, U.C.C. Article 9 includes a filing system for use in "communicating the existence of a lien from the holder to a person who is considering becoming a creditor of the same debtor."[109] The goal of the filing system is to give prospective creditors actual knowledge of preexisting liens.[110] Unfortunately, "filing systems are highly imprecise and difficult and expensive to use," particularly for those searching the system for evidence of preexisting liens.[111] The expense and difficulty of using such filing systems stem, at least in part, from the fact that: (1) there is not just one filing system, but many;[112] (2) "search methods differ widely from one filing system to another";[113]

105. *Id.*
106. When considered in the context of this broader theory, my prior proposal to use DLT to regulate DLT was a proposal for a crypto-legal structure, which, when taken together with other crypto-legal structures created across any other number of substantive disciplines, will create a new legal discourse of cryptolaw.
107. U.C.C. § 9-109, *reprinted in* CAROL L. CHOMSKY ET AL., SELECTED COMMERCIAL STATUTES 737–43 (2016).
108. Lynn M. LoPucki, *Computerization of the Article 9 Filing System: Thoughts on Building the Electronic Highway*, 55 L. & CONTEMP. PROBS. 5, 5 (1992).
109. LOPUCKI ET AL., *supra* note 100, at 281.
110. *Id.*
111. *Id.* at 281–82.
112. *Id.* at 283.
113. *Id.* at 294.

(3) searches cannot be conducted on the full text of the filings, but rather, only on the index of the filing, which itself is limited to a single piece of information—the debtor's name;[114] (4) filings in the system remain effective even after the name of the debtor listed on the filing has changed or the corporate debtor has undergone a structural change;[115] and (5) following the rules of lapse and continuation to ensure a security interest is not lost remains complicated.[116] In terms of the DLT services bundle, the common element among these five problems with the Article 9 filing system is that the parties using the system can never be certain that the facts that they are looking at are the same facts that the other parties in the system see. In other words, the system regularly fails to reach a consensus about the existence and evolution of shared facts. This makes the U.C.C. Article 9 filing system ripe for reform using crypto-legal structures that balance the proportion of the five DLT services—consensus, validity, uniqueness, immutability, and authentication—in ways that serve the unique goals of the filing system. For example, although the Article 9 filing system would likely benefit from the full robustness of consensus as public DLT systems, perhaps only the debtor, secured creditor, and the filing office need to validate the financing statements that pertain to specific transactions, rather than all the users of the crypto-legal structure (as would be the baseline for permissionless DLT).

Another area of the law that similarly appears to be ripe for the application of DLT, albeit to address a different problem in the law, is the anti-money laundering (AML) regulations implemented pursuant to the federal Bank Secrecy Act (BSA).[117] The BSA and its implementing regulations (the BSA Regulations) are enforced by the Financial Crimes Enforcement Network of the United States Department of the Treasury (FinCEN).[118] The BSA Regulations, an AML regime, require covered entities to know their customers and report transactions that

114. *Id.* at 295. I recognize that this is only an introductory list of the failings of the Article 9 filing system. A full list is beyond the scope of this Article and has been considered extensively by the literature and cases on Article 9. For a summary of those literature and cases, see LoPucki, *supra* note 108, at 6–15.

115. LoPucki, *supra* note 108, at 23.

116. *Id.* at 24.

117. In fact, the Directorate General of Financial Stability, Financial Services, and Capital Markets Union (FISMA) of the European Commission appears to concur, as it is conducting a feasibility study of whether blockchain technology can lower compliance obligations for financial institutions. DIEDRICH, *supra* note 8, at 65.

118. Bank Secrecy Act tits. I–II, Pub. L. No. 91-508, 84 Stat. 1114, 1114–24 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951–59; 31 U.S.C. §§ 5311–14, 5316–32 (2012)) (authorizing the Secretary of the Treasury to issue regulations requiring organizations falling within the definition of "financial institutions" to keep records and file certain reports).

are either suspicious or surpass a certain volume threshold.[119] As part of the AML structure, the Funds Transfer[120] and Funds Travel[121] rules require covered entities to pass certain information about the parties involved in a transmittal of funds to the receiving institution together with the funds transferred during the transaction.[122]

To comply with the BSA Regulations, covered entities register with FinCEN and implement business-specific controls designed to flag suspicious transactions and then report flagged transactions to FinCEN on the prescribed forms.[123] This AML system suffers from at least two major flaws: (1) even a diligent company may not red flag all transactions that qualify for reporting under the BSA Regulations, and (2) regular enforcement by FinCEN takes place through onsite inspections of books and records on an infrequent basis unless an entity is deemed such a risk that it should be investigated extensively and prosecuted for the crime of failing to comply with the BSA Regulations.[124] At the root of these problems lies an inability to automatically identify the shared facts of interest that trigger compliance obligations. In other words, the system regularly fails to reach a consensus about the existence and evolution of shared facts. This makes BSA Regulation compliance a legal area ripe for the application of crypto-legal structures.

Thus far, then, cryptolaw can be conceptualized as a new area of legal discourse used to identify when crypto-legal structures should be adopted to address situations where the law struggles to provide a suitable mechanism for actors to reach a consensus about the existence and evolution of shared facts. Each crypto-legal structure represents law implemented and delivered through DLT-based computer code. The next step in conceptualizing cryptolaw is identifying the method or methods by which crypto-legal structures will be adopted.

---

119. *See* 31 C.F.R. § 1010.620 (2013) (requiring covered financial intuitions to create know-your-customer, or due diligence, programs); 31 C.F.R. § 1022.310 (2013) (reporting currency transactions over ten thousand dollars); 31 C.F.R. § 1022.320 (2013) (reporting suspicious transactions).

120. 31 C.F.R. § 1010.410(e) (2013).

121. § 1010.410(f).

122. *See generally* FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREASURY, FINCEN ADVISORY: FUNDS TRANSFERS (1996), https://www.sec.gov/about/offices/ocie/aml2007/fincen-advsiii.pdf [https://perma.unl.edu/W35R-SAVK].

123. For registration and renewal requirements, see 31 U.S.C. § 5330 (2012) and 31 C.F.R. § 1022.380 (2013). For requirements concerning the development and execution of an AML program that implements reporting obligations, see 31 U.S.C. § 5318(a)(2) (2012) and 31 C.F.R. § 1022.210 (2013).

124. 31 U.S.C. § 5318(h) (2012) (requiring an independent review to "test, monitor and maintain, its anti-money laundering program" without further details). The frequency and extent of the review is determined in accordance with the MSB's risk-assessment profile. *Id*.

B. Three Possible Methods of Adopting Crypto-Legal Structures

There are three ways in which crypto-legal structures seem likely to emerge: (1) through industry-constructed crypto-legal structures later adopted by government actors, (2) through crypto-legal structures directly coded and adopted by government actors, and (3) through international development of crypto-legal structures.[125] Furthermore, more than one single crypto-legal structure could be created to deal with a specific problem to more endogenously meet the needs of the governed. For example, in the context of compliance with the BSA Regulations, the crypto-legal structures useful for large, federally chartered banks are likely to look different from those useful to small FinTech companies that often prefer to incorporate elements of permissionless DLT into their business models. The crypto-legal structures would work together and in tandem, and could call to each other, leading to the development of more complex, nimble, and responsive crypto-legal structures over time. More fully understanding the importance and likelihood of each of the possible pathways for adopting crypto-legal structures calls for a closer examination of each in the context of one or both of the real-world legal examples set forth above.

1. Government Adoption of Industry-Created Crypto-Legal Structures

Crypto-legal structures might be constructed voluntarily by the business community relying upon DLT when the community identifies an opportunity to endogenously implement cryptolaw at the level of permissionless DLT protocols.[126] For example, the Bitcoin blockchain core developers have already undertaken a version of this process for certain legal rules of particular concern to the community: AML compliance under the BSA. In the summer of 2016, the Bitcoin blockchain core developers released BIP 75, a technical standard for use in connection with payments applications running on the Bitcoin blockchain.[127] BIP 75 both enables businesses to offer a more user-

125. In each case, the government agency would adopt the crypto-legal structure either by issuing guidance interpreting the crypto-legal structure as complying with existing requirements or by issuing code or proof-of-concept as part of a rulemaking process subject to a public notice-and-comment period.

126. Reyes, *supra* note 19, at 230–31.

127. *See* Kyle Torpey, *BIP 75 Simplifies Bitcoin Wallets for the Everyday User*, BITCOIN MAG. (Apr. 23, 2016), https://bitcoinmagazine.com/articles/bip-simplifies-bitcoin-wallets-for-the-everyday-user-1461856604 [https://perma.unl.edu/F5MC-BNU3].

friendly interface and comply with certain anti-money-laundering laws overseen by FinCEN.[128]

One of the key authors of BIP 75, Justin Newton, described the protocol as an opportunity to accept the fact that AML and know-your-customer rules apply to certain bitcoin payments applications, while creating a compliance mechanism that "protects fungibility, privacy and the open, permissionless nature of Bitcoin."[129] Newton went on to affirm the primary benefits of creating such crypto-legal structures, namely, making them endogenous in nature, saying, "In the absence of a standard that encourages those values, we will end up with hidden systems that do exactly the same thing, but without taking the concerns of the community into account."[130] BIP 75 is an example of an endogenously created crypto-legal structure.[131] To graft BIP 75 into an emerging body of cryptolaw, FinCEN could adopt a regulation providing that companies applying BIP 75 to their payments services will be deemed compliant with certain anti-money-laundering rules if,

128. *Id.* BIP 75 is referred to colloquially as "the Payment Protocol" and "creates a method of communication between a merchant and their customers before a payment is made." *Id.* The benefit of this communication mechanism is that it "allows customers to see human-readable payment destinations, which can be authenticated via digital signatures." *Id.* It also "creates a proof-of payment for the customer" and enables a refund mechanism. *Id.* These are all elements of BIP 75 that make bitcoin transactions more user-friendly. BIP 75 also "make[s] it easier for companies (financial in nature or not) to collect data on their customers." Kyle Torpey, *Does BIP 75 Really Threaten Bitcoin's Fungibility?*, BITCOIN MAG. (June 30, 2016) [hereinafter Torpey, *BIP 75 and Fungibility*], https://bitcoinmagazine.com/articles/does-bip-really-threaten-bitcoin-s-fungibility-1467302909 [https://perma.unl.edu/7HTS-BAQA]. Such data collection will enable compliance with such anti-money-laundering rules as the Funds Transfer and Funds Travel Rules administered by FinCEN, which require financial institutions to transfer data between them relating to the senders and receivers of funds transfers. 31 C.F.R. § 1010.410(e)–(f) (2013).

129. Torpey, *BIP 75 and Fungibility*, *supra* note 128 (quoting Justin Newton).

130. *Id.* (quoting Justin Newton).

131. Other voluntary organizations formed by the DLT industry are also working to create technical standards that could be adopted as crypto-legal structures by the appropriate regulatory authority. For example, the World Wide Web Consortium (W3C) is considering whether to design technical standards for the compatibility of DLT and web applications. W3C, BLOCKCHAINS AND THE WEB REPORT (2016), https://www.w3.org/2016/04/blockchain-workshop/report.html [https://perma.unl.edu/DTK3-LKKQ]. Further, the Chamber of Digital Commerce established the Blockchain Alliance, a forum for promoting collaboration between law enforcement and the blockchain community to build standards for cooperation and investigation. *Blockchain Alliance*, CHAMBER DIGITAL COM., http://digitalchamber.org/blockchain-alliance.html [https://perma.unl.edu/GW49-LEQN]. In addition, the Coalition of Automated Legal Applications serves as the Internet Governance Forum's Dynamic Coalition for the governance of blockchain technologies. COALA, DYNAMIC COALITION ON BLOCKCHAIN TECHNOLOGIES 3 (2016), https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/4189/125 [https://perma.unl.edu/4Z7M-VGDQ].

for example, the companies submit to a technical audit process not less than two times per calendar year. To do so, FinCEN would engage in a rule-making process, subject to a public notice-and-comment period. Alternatively, FinCEN might issue administrative guidance interpreting BIP 75 as a program feature that complies with certain elements of the BSA Regulations. The possibility of industry-developed crypto-legal structures enables new forms of regulatory entrepreneurship[132] and thereby offers an organic process for narrowing the gap between law and technology.

2. Crypto-Legal Structures Directly Coded by Government

The proliferation of permissioned ledgers, and the admitted reticence of the core DLT developers to endogenously adopt standards such as BIP 75,[133] ensures the importance of the second method for creating and implementing crypto-legal structures: government creation of crypto-legal structures. In this second method, the relevant government agency, employing their own in-house software developers, will design the crypto-legal structure, issue it as a regulation through the public rule-making process, or declare it compliant by interpreting existing regulations in administrative guidance. In the context of large federally regulated financial institutions' compliance with the BSA Regulations, this type of crypto-legal structure may be more useful than BIP 75. Further, it builds on a trend with which such institutions are already familiar; namely, RegTech, the process of trying to automate BSA compliance with technology that prefills and files the required FinCEN forms when algorithms spot certain red flags.[134] A crypto-legal structure for BSA Regulations would merely be the next step in technological evolution for efficient and accurate implementation of the law, with the advantages of increased efficiency gains, decreased costs of enforcement, and decreased false positives over its predecessor RegTech solutions. For example, the U.S. Department of Health and Human Services is exploring the use of blockchain for

132. Pollman & Barry, *supra* note 101, at 384–85 (defining regulatory entrepreneurship as a class of business activity in which a company "makes changing the law a material part of its business plan" because its financial success depends "on the resolution of legal issues concerning a core aspect of [its] business").

133. Torpey, *BIP 75 and Fungibility*, *supra* note 128 ("BIP 75 institutionalizes [regulatory compliance] in a convenient way that everyone can easily use and expect. We should comply with AML [and] KYC [regulations] only grudgingly." (alteration in original) (quoting lead Blockchain developer Peter Todd)).

134. DELOITTE, REGTECH IS THE NEW FINTECH: HOW AGILE REGULATORY TECHNOLOGY IS HELPING FIRMS BETTER UNDERSTAND AND MANAGE THEIR RISKS (2016), https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_2016_FS_RegTech_is_the_new_FinTech.pdf [https://perma.unl.edu/KQH5-3BED].

managing health data,[135] and the European Union is considering blockchain for financial regulation.[136]

Crypto-legal structures coded directly by the relevant regulatory agency would also be useful in the context of improving legal structures that depend upon a filing system of some kind, such as the U.C.C. Article 9 example discussed above, among others.[137] In fact, a variety of regulatory agencies and legislative bodies already recognize potential uses for such crypto-legal structures.[138] Using crypto-legal structures in this context would increase efficiencies, decrease transaction costs, and decrease problems related to the exchange of asymmetrical information. Using a crypto-legal structure in Article 9 and similar contexts also offers the added benefit of enabling regulators to continue to require compliance with jurisdiction-specific rules while also maintaining a national (or international) filing system without significantly increasing regulatory burden. This possibility is ensured by the fact that as long as the crypto-legal structures comply with a minimum and uniform standard for interoperability and compatibility, the crypto-legal structures could be designed to interact with each other across borders and across systems.

3. International Development of Crypto-Legal Structures

The concern for interoperability and compatibility of the various crypto-legal structures that will emerge leads to a third process for their creation and implementation: international standard setting. This process would perhaps evidence characteristics directly opposite

135. Bradley, *supra* note 13; Press Release, U.S. Dep't of Health & Human Servs., ONC Announces Blockchain Challenge Winners (Sept. 1, 2016), https://wayback.archive-it.org/3926/20170127190114/https://www.hhs.gov/about/news/2016/08/29/onc-announces-blockchain-challenge-winners.html [https://perma.unl.edu/JUF7-5V45].

136. DIEDRICH, *supra* note 8, at 19.

137. *See supra* notes 107–16 and accompanying text for a U.C.C. Article 9 example. For another example of a solution that is bein.g developed by IBM, see developerWorks TV, *IBM Blockchain Car Lease Demo*, YOUTUBE (Mar. 1, 2016), https://www.youtube.com/watch?v=IgNfoQQ5Reg.

138. *See, e.g.*, del Castillo, *supra* note 12; Stan Higgins, *Vermont Is Close to Passing a Law that Would Make Blockchain Records Admissible in Court*, COINDESK (May 17, 2016), http://www.coindesk.com/vermont-blockchain-timestamps-approval [https://perma.unl.edu/M2U4-7L68]; Giulio Prisco, *Delaware Blockchain Initiative to Streamline Record-Keeping for Private Companies*, BITCOIN MAG. (May 9, 2016), https://bitcoinmagazine.com/articles/delaware-blockchain-initiative-to-streamline-record-keeping-for-private-companies-1462812187 [https://perma.unl.edu/8YP4-KDS6]; Rizzo, *supra* note 11; Andrea Tinianow & Caitlin Long, *Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Mar. 16, 2017), https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance [https://perma.unl.edu/TF6D-6E3A].

to that of crypto-legal structures created by DLT core developers in that it will be slow and bureaucratic. The reality is, however, that as a technology with global reach, crypto-legal structures may emerge internationally as a preferred form of legal implementation and adjudication, and in such a scenario, only international cooperation will ensure that industry is not trapped in a clash of crypto-legal structures which would render them unable to operate without redesigning the code underlying their service in each jurisdiction.

Tellingly, the initial steps in this process are already underway. In April 2016, Australia's national standard-setting body proposed that the International Standards Organization (ISO) create a new field of technical activity to develop the "[s]tandardi[z]ation of blockchains and distributed ledger technologies to support interoperability and data interchange among users, applications and systems."[139] Although the field of activity will specifically exclude "legal obligations and regulatory matters addressed by government jurisdictions," one of the work's articulated goals is to assure interoperability and compatibility across DLT and across jurisdictions such that individual jurisdictions may "work towards a regulatory framework that provides a mix of legal and technical rules."[140] In other words, the stated aim of the ISO process is to pave the way for national jurisdictions to begin implementing crypto-legal structures for their individual jurisdictions.

Over time, other areas of the law that would benefit from a shared record of tamper-resistant, verifiable, and authenticated facts will become evident. As crypto-legal structures develop to address those problems, the crypto-legal structures may be designed to interact with each other, to interact with private contracting parties,[141] or to interact with the governed without a government intermediary. As smart-contract coding capacity increases, we can imagine more complex crypto-legal structures with more autonomous and self-executing features. Crypto-legal structures might be supplemented by other technology, such as predictive technology[142] or data-mining technology,[143]

139. STANDARDS AUSTL., ISO, FORM 1: PROPOSAL FOR A NEW FIELD OF TECHNICAL ACTIVITY (2016), https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Links%20Within%20Stories/ISO%20TSP%20258%20%28Blockchain%20and%20Electronic%20Distributed%20Ledger%20Technologies%29.pdf [https://perma.unl.edu/G6RU-GPL4].

140. *Id.*

141. This potential becomes particularly interesting if a private law of *lex cryptographia* emerges amongst peer-to-peer merchants acting over DLT, as suggested by Aaron Wright and Primavera De Filippi. Wright & De Filippi, *supra* note 19. Under such circumstances, cryptolaw may enable fluid transitions and interactions between public and private law that have not previously been possible (or at least have been impossible to document to date).

142. For a discussion of the implications of predictive technology for the law generally, see Casey & Niblett, *supra* note 16. And for a discussion of the implications of

such that the smart contracts are able take on predictive qualities and decisional capabilities. As the number of crypto-legal structures, the frequency of their interactions with each other, and the complexity of their designs increase, cryptolaw, the study of and discourse regarding these interactions and complexities, begins to crystalize into a separate and increasingly important area of law. A legal system in which crypto-legal structures begin to take root will see fundamental changes in the way the governed—whether individuals or entities—experience, understand, and relate to the law.

C. More than Just Another "Law of the Horse"

Conceived of as the study of and discourse regarding interlinked legal structures represented by self-executing, smart-contracting, semi-autonomous, cryptographic computer code, the cryptolaw proposed here represents something fundamentally different from the way that term has been sparingly and tentatively used to date.[144] At present, most discussions about an emerging and evolving law of DLT mostly revolve around whether new, improved, or different regulation is required by the cryptographic nature of DLT.[145] Such discussions

---

predictive technology in the credit-score context specifically, see Citron & Pasquale, *supra* note 17.

143. For a discussion of the possible implications of data-mining technology for the law, see Kaal & Vermeulen, *supra* note 15.

144. The most similar use of the term to date is by one of the chief developers of the Ethereum protocol, Gavin Wood, who explained:

> Around the 1990s it became clear that algorithmic enforcement of agreements could become a significant force in human cooperation. Though no specific system was proposed to implement such a system, it was proposed that the future of law would be heavily affected by such systems. In this light, Ethereum may be seen as a general implementation of such a *crypto-law* system.

GAVIN WOOD, ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER 2, http://gavwood.com/Paper.pdf [https://perma.unl.edu/7N3T-7SER]. However, Dr. Wood's conception of cryptolaw stems from an entirely code-based perspective and does not tie the use of code in Ethereum to the existing legal system. In other words, Dr. Wood's article is an attempt to fill the gap left by the fact that "no specific system was proposed to implement" cryptolaw by either Dr. Wood or his predecessor Nick Szabo. *Id.* Other references to "crypto law" really intend to refer to the law governing encryption technologies, usually with reference to export controls relating to cryptography. *See, e.g.*, BERT-JAAP KOOPS, CRYPTO LAW SURVEY (1995), http://coast.cs.purdue.edu/pub/doc/cryptography/Crypto_Law_Survey/CryptoLawSurvey.html [https://perma.unl.edu/8TKA-YJNV] (reporting a "survey of cryptography laws"). For a good primer on the laws governing cryptography, see Nathan Saper, Note, *International Cryptography Regulation and the Global Information Economy*, 11 NW. J. TECH. & INTELL. PROP. 673 (2013). A few members of the DLT community refer to crypto law to refrence "legal issues in cryptocurrency." *See, e.g.*, CRYPTO LAW BLOG, https://cryptolawblog.wordpress.com [https://perma.unl.edu/3H3E-69GU].

145. I would include my own initial consideration of the subject in this category. As I argued there, Reyes, *supra* note 19, these conversations are an important initial

do not actually contemplate the emergence of new legal structures using DLT. Furthermore, such discourse has led to accusations that cryptolaw is no more than a cyberlaw redux because it mirrors discussion of cyberlaw in the early Internet days, in which the debate focused on who and how to regulate the Internet.[146] Cyberlaw is largely viewed today as an area of law for which there is "no unanimity" and for which "a list of issues substitutes for an abstract definition."[147] Today, the term "cyberlaw" is synonymous with "the area of Internet regulation."[148] In other words, "the vast majority of cyberlaw analysis focuses on the application of existing legal norms—intellectual property, trademark, antitrust, content regulation and the like—to cyberspace issues."[149] As such, cyberlaw has been compared to "the law of the horse."[150] Judge Frank Easterbrook saw activity in cyberspace, like the ownership and management of horses, as a specialized endeavor to which general legal rules could be applied as problems arose on a case-by-case basis.[151] As a result, Easterbrook argued that "[a]ny effort to collect these strands into a course on 'The Law of the Horse,'" or a law of cyberspace, "is doomed to be shallow and to miss unifying principles."[152]

Several commentators prominently countered that cyberlaw could avoid its apparent fate as the law of the horse by focusing on the ele-

---

step to enable those using the technology in business models at present the regulatory certainty required to operate while innovating. The argument here is that while that discussion remains an important first step, the conversation should not, and need not, end with consideration of how to regulate DLT. *Id.*

146. Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 606–07 (2003).

147. *Id.* at 606 n.1.

148. *Id.* at 606.

149. *Id.* at 608; *see* Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145, 1147–49 (2000); *see also* Needham J. Boddie, II et al., *A Review of Copyright and the Internet*, 20 CAMPBELL L. REV. 193, 193–94 (1998) ("The expansion of the Internet in size, usage and influence has generated a variety of novel legal questions. . . . [Nonetheless,] 'Internet Law' does not represent a new field or body of law such as tort law, contract law or property law. Internet Law is more or less the application of existing legal doctrines to the new technologies, avenues of commerce, and means of human interaction defined, created and experienced on the Internet."); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1379–1400 (1996) (prescribing application of distinct laws to cyberspace); Allison Roarty, *Link Liability: The Argument for Inline Links and Frames as Infringements of the Copyright Display Right*, 68 FORDHAM L. REV. 1011, 1011 (1999) ("As the Internet continues to expand exponentially, so do the corresponding legal issues."); Steven R. Salbu, *Who Should Govern the Internet?: Monitoring and Supporting a New Frontier*, 11 HARV. J.L. & TECH. 429, 430 (1998) (reviewing the many different cyberlaw issues that have received significant attention).

150. Easterbrook, *supra* note 93, at 207–08.

151. *Id.*

152. *Id.* at 207.

ments that make cyberspace unique: the concept of cyber-structure, or "the indirect regulation of cyberspace through technological standards and structures."[153] Most prominently, Professor Lawrence Lessig argued that examining the interaction between law and cyberspace teaches "about the limits on law as a regulator and about the techniques for escaping those limits" and requires a close look at "the collection of tools that a society has at hand for affecting constraints upon behavior."[154] Lessig concluded that, with the emergence of cyberspace, a new regulatory force emerged—the computer code that makes interaction in cyberspace possible.[155] Tying cryptolaw to this literature reveals that, to prevent cryptolaw from being summarily dismissed as another law of the horse, discussion of cryptolaw cannot end with whether and how to regulate DLT. If the discussion ends there, cryptolaw will devolve into a group of loosely affiliated musings about how to adapt legal paradigms built on assumptions of trusted and regulateable intermediaries to the world of DLT, which relies on math and inherently distrusts intermediaries.[156] Instead, this Article

153. Mayer-Schönberger, *supra* note 146, at 608–09.

154. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999) [hereinafter Lessig, *The Law of the Horse*].

155. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) [hereinafter LAWS OF CYBERSPACE I] ("That regulator is the obscurity in the book's title—*Code*. . . . In cyberspace we must understand how code regulates—how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is. As William Mitchell puts it, this code is cyberspace's 'law.' *Code is law*." (footnote omitted)); Lessig, *The Law of the Horse*, *supra* note 154, at 549 ("[M]ore than law alone enables legal values, and law alone cannot guarantee them. If our objective is a world constituted by these values, then it is as much these other regulators—code, but also norms and the market—that must be addressed.").

156. The comparison between the current literature on DLT and much of the cyberlaw literature is not unwarranted. The cyber-governance discussions regarding whether and how to regulate the Internet centered around four typical positions, Mayer-Schönberger, *supra* note 146, at 612 (outlining three of the positions), each of which has a counterpart in the DLT-governance literature prevalent to date. The first position, which one commentator named the state-based traditionalists, argued that the nation-state has the authority to regulate cyberspace in the same manner that it has the authority to regulate any other space. *Id.* at 612–18. The DLT-governance version of the state-based traditionalist position grounds itself in real-life events and argues that the state, by regulating applications running on DLT, is effectively regulating DLT in the same manner that it regulates any other space. *See, e.g.*, Rhys Bollen, *The Legal Status of Online Currencies: Are Bitcoins the Future?*, 24 J. BANKING & FIN. L. & PRAC. 272, 279 (2013) (arguing that "Bitcoins are a form of intangible private property, a valuable digital artefact" and are therefore "analogous with other forms of intangible private property, such as digital music, shares, licenses, trademarks, copyright, goodwill, domain names, frequent flier points and brands"); J. Scott Colesanti, *Trotting Out the White Horse: How the S.E.C. Can Handle Bitcoin's Threat to American Investors*, 65 SYRACUSE L. REV. 1, 38 (2014); Nelson DaCunha, *Virtual Property, Real Concerns*, 4 AKRON INTELL. PROP. J. 35, 41 (2010) (noting that if decentralized virtual currencies are a form of intangible property, tort law offers one way to protect interests of both users and service providers); Ruoke Yang, *When Is*

demonstrates that cryptolaw is properly conceived of as a new way of thinking, studying, and talking about the law that anticipates the new issues arising from implementing law through cryptographic, smart-contracting computer code with the capacity for self-execution, embedded predictive technology, and autonomous interaction. As such, cryptolaw is much more than just another law of the horse.

As was true of Professor Lessig's focus on cyber-structures (e.g., the code), when the true focus of cryptolaw lies in DLT's unique capacity for creating new crypto-legal structures, cryptolaw disrupts the way we currently think about the law and regulation. Specifically, DLT has the potential to take the cyberstructural elements of cyberlaw and pursue them to an extreme version of code as law through crypto-legal structures. In other words, DLT offers lawmakers the capacity to actually write law into computer code, embed smart contracts to make the code self-executing, and embed predicative and machine-learning technology to enable the law to learn and adapt as it executes. DLT thereby offers an opportunity to resolve some of the very objections Easterbrook originally made to the idea of a law of cyberspace: crypto-legal structures allow the law, written into

---

Bitcoin a Security Under U.S. Securities Law?, 18 J. TECH. L. & POL'Y 99, 108 (2013). The second position, dubbed the cyber separatists, advocated that no regulation be imposed and that cyberspace be left to self-regulation. Mayer-Schönberger, *supra* note 146, at 618–26. A variety of DLT researchers and industry actors similarly plead for regulatory caution, arguing that self-regulation would be better poised to encourage innovation when DLT is still so new and unknown. *See, e.g.*, Wright & De Filippi, *supra* note 19. The third cyber-governance position, referred to as the internationalists, claimed that in light of the international nature of the technology, governance would only be appropriate at an international level through international law. Mayer-Schönberger, *supra* note 146, at 626–30. The international, borderless, inherently decentralized nature of DLT has also given rise to arguments that only international bodies should have the authority to dictate DLT-governance structures. *See e.g.*, Nicholas Plassaras, Comment, *Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF*, 14 CHI. J. INT'L L. 377 (2013). The fourth position, offered as an alternative to each of the other three, argued that a layered architectural approach was more appropriate and encouraged lawmakers to layer regulation in ways that took advantage of the uniqueness of the technology. Mayer-Schönberger, *supra* note 146, at 637–40. Similarly, alternative regulatory approaches, rooted in the layers and architectural principles developed in the Internet context, have been suggested for use in DLT governance. Daniel Folkinshteyn, Mark M. Lennon & Timothy Reilly, *A Tale of Twin Tech: Bitcoin and the WWW*, 10 J. STRATEGIC & INT'L STUD. 82 (2015). Both the cyber-governance debate and the DLT-governance debate center on how current law can and should be applied to the emerging technology of the time, arguably allowing the current DLT literature to fall victim to the law-of-the-horse critique. As this Article has demonstrated, however, cryptolaw possesses the potential to move beyond the DLT-governance debate to a consideration of the potential impact of the technology at issue on the very foundations of law and how society understands law.

ever-adapting code,[157] to endogenously keep pace with rapidly developing changes in technology.[158] Ultimately then, DLT offers more than merely emerging technology that poses new and interesting legal questions, but rather, it offers a technology that can be employed to form an entirely new discourse on the law—cryptolaw.

IV. CONCEPTUALIZING CRYPTOLAW AS DISRUPTIVE LEGAL DISCOURSE

Implementing crypto-legal structures will disrupt national legal systems at their core, disrupting the very way we study, think, and talk about the law. The core affected elements include legal structure, substantive law, and legal culture.[159] Crypto-legal structures will disrupt each of these elements, causing fundamental change to any legal system in which they are employed. This Article uses the comparative legal method as a methodological paradigm for conceptualizing the contours of the new legal discourse that will result from using DLT to implement law in a disciplined way. Comparative law has been described as the "critical method of legal science" because of its focus on "the juxtaposing, contrasting and comparing of legal systems or parts thereof with the aim of finding similarities and differences."[160] The comparative enterprise takes place at both the macro and micro level.[161] At the macro level, comparative law uses an investigation of similarities and differences to further "the universal knowledge and phenomena of law."[162] At the micro level, the goal of comparative law

157. LAWS OF CYBERSPACE I, *supra* note 155, at 109 ("Code is not constant. It changes.").

158. As a supplement to his argument that general legal rules were sufficient to address issues arising in cyberspace, Easterbrook also claimed that attempting to create a law of new technology was inappropriate because the law could not keep pace:

> If we are so far behind in matching law to a well-understood technology such as photocopiers—if we have not even managed to create well-defined property rights so that people can adapt their own conduct to maximize total wealth—what chance do we have for a technology such as computers that is mutating faster than the virus in *The Andromeda Strain*?

Easterbrook, *supra* note 93, at 210.

159. *See, e.g.*, LAWRENCE M. FRIEDMAN, LAW AND SOCIETY 6–9 (1977) [hereinafter FRIEDMAN, 1977]; LAWRENCE M. FRIEDMAN, THE LEGAL SYSTEM 11–16 (1975) [hereinafter FRIEDMAN, 1975]; Lawrence M. Friedman, *Legal Culture and Social Development*, 4 LAW & SOC'Y REV. 29 (1969); Lawrence M. Friedman, *On Legal Development*, 24 RUTGERS U. L. REV. 11 (1969).

160. Esin Örücü, *Developing Comparative Law*, *in* COMPARATIVE LAW: A HANDBOOK 43, 44 (Esin Örücü & David Nelken eds., 2007).

161. Gerhard Dannemann, *Comparative Law: Study of Similarities or Differences?*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 383, 387 (Mathias Reimann & Reinhard Zimmermann eds., 2006).

162. Örücü, *supra* note 160, at 46.

is to aid foreign-law research, promote law reform, and facilitate better understanding of other legal systems.[163] Because the micro-comparison goals of promoting legal reform and better understanding other legal systems directly intersect with the prospect of implementing new and existing legal structures through crypto-legal structures wherein DLT operates as a type of foreign legal system, this Article applies elements of comparative micro-analysis to examine the implications of crypto-legal structures for the legal system, including: comparative study of legal cultures, the study of legal transplants, and functional comparison.[164] With those methodological tools in hand, this Part first considers the potential effect of crypto-legal structures on existing substantive law, arguing that they simultaneously offer a path for simplifying law through functional equivalents in the code and lead to the emergence of new regulatory actors. This Part next argues that, over time, the resulting subtle shifts in substantive law will lead to broader changes in the legal structures that comprise the system. This Part concludes by considering how those changes in legal structure will impact current legal culture by altering the scope of the relevant legal actors.

A. Disruption of Substantive Law

The term substantive law refers to both "the substantive rules and rules about how institutions should behave."[165] If DLT is approached as a form of foreign law, the creation of a crypto-legal structure by taking an existing legal rule and rewriting it into computer code should be approached as an exercise in legal transplantation. Legal transplantation is the process of taking a legal artifice from its home jurisdiction and implementing it in a foreign, receiving jurisdiction. Unless legal transplants are "designed to deal effectively with the special characteristics of the recipient jurisdiction,"[166] in this case DLT, the transplanted law can have unexpected effects.[167] Even when a transplanted law has unexpected effects, it succeeds if it achieves its function in the receiving jurisdiction.[168] Understood in that light, any consideration of legal transplants must exist alongside, and in relation

163. *Id.*
164. Ralf Michaels, *The Functional Method of Comparative Law*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW, *supra* note 161, at 339, 341.
165. FRIEDMAN, 1975, *supra* note 159, at 14. Friedman goes on to say that "[a] legal system is the union of 'primary rules' and 'secondary rules.' Primary rules are norms of behavior; secondary rules are norms *about* those norms—how to decide whether they are valid, how to enforce them, etc." *Id.* (footnote omitted).
166. Michael S. Gal, *The "Cut and Paste" of Article 82 of the EC Treaty in Israel: Conditions for a Successful Transplant*, 9 EUR. J.L. REFORM 467, 469 (2007).
167. *Id.*
168. *Id.* at 472 ("I suggest defining success as the ability of the transplanted law to achieve its goals in the transplanting country.").

to, the comparative-law functional method.[169] The functional method of comparative law considers elements of a legal system in light of the function that it serves in responding to a societal problem.[170] In so doing, the functional method recognizes that other systems may use functional equivalents, "other institutions, legal or non-legal, that perform the same function," to address the same societal problem differently.[171] In other words, the first step in the transplantation process is to identify a problem ripe for change through transplantation, here a legal structure that would benefit from consensus on the existence of shared facts through importation of the law into DLT-based computer code. Then the transplantation process requires a consideration of any institutions or elements of the receiving system, here the DLT, that serve some or all of the same function. Only then can the transplant, the crypto-legal structure, be successfully designed.

As a series of legal transplants from existing law into the foreign system of DLT, the emergence of crypto-legal structures will disrupt substantive law in at least three ways. First, crypto-legal structures will enable the simplification of many legal rules using existing functional equivalents in the DLT during the process of coding crypto-legal structures. Second, building crypto-legal structures, as a form of legal transplantation, will lead to the emergence of new regulatory agents: certain self-executing elements of the code and the developers that code the law into crypto-legal structures. Finally, crypto-legal structures will give rise to new questions for adjudication.

1. Simplification of Substantive Law

Comparative law's functional method offers methodological tools for recognizing that "different legal rules can play similar functions in different societies."[172] Functionalist comparative law compares legal

169. *Id.* ("Several conditions for a successful transplant have been identified in the literature. . . . Although Watson generally focused on whether a transplant will occur or not, he implicitly identified several factors that contribute to a successful transplant. Most importantly, he emphasized the importance of the idea behind the law. If the idea is a good one, in that it serves to provide a suitable solution for a legal problem, then the transplant will have higher chances of success. Yet as many commentators have emphasized, for this condition to be fulfilled the idea should be a good one in light of the special conditions of the transplanting jurisdiction." (footnote omitted) (citing Alan Watson, *Comparative Law and Legal Change*, 37 CAMBRIDGE L.J. 313, 324–26 (1978))).

170. Ralf Michaels, *The Functionalism of Legal Origins*, *in* DOES LAW MATTER? ON LAW AND ECONOMIC GROWTH 21, 23 (Michael Faure & Jan Smits eds., 2011).

171. Ralf Michaels, *Comparative Law by Numbers? Legal Origins Thesis,* Doing Business *Reports, and the Silence of Traditional Comparative Law*, 57 AM. J. COMP. L. 765, 778 (2009).

172. Tom Ginsburg, *Lawrence M. Friedman's Comparative Law, with Notes on Japan*, 5 J. COMP. L. 92, 102 (2010) (citing R. ZWEIGERT & H. KOTZ, AN INTRODUCTION TO COMPARATIVE LAW (2d ed. 1998)).

systems by focusing on facts, such as the effects of rules, events, and judicial responses or decisions in response to real-life situations.[173] Functionalist comparative law then considers these comparisons in light of "the theory that [comparative law's] objects must be understood in the light of their functional relation to society."[174] Together, these two facets of functionalist comparative law allow for the identification of functional equivalents between two systems, that is, the identification of institutions in each system that, even if doctrinally different and even if one is a legal institution while the other is a non-legal institution, fulfill similar functions.[175]

The idea of focusing on the function of an institution is not unique to comparative law. In fact, the field of computer programming uses a similar analytical approach, referred to as "systems analysis."[176] Similar to the comparative-functional method, "[s]ystems analysis proceeds by identifying systems, discovering their goals or attributing goals to them, mapping their subsystems and the functions each performs, determining their internal structures, depicting them with attention paid to efficiency of presentation, and searching for internal inconsistencies."[177] The similarities between the two approaches give regulators, armed with functionalist-comparative-law theory, and DLT computer coders, armed with system analysis, common ground for first assessing a specific existing legal structure, identifying its functional relation to society, breaking out subsystems of the legal structure, and identifying their functions, and then assessing which elements of DLT, if any, endogenously fill those functions. Where DLT does, or can be coded to, fill certain functions of the law, the substantive law can be simplified as it is translated into a crypto-legal structure.

Further analysis of the Article 9 filing system illustrates the impact of translating existing legal structures into crypto-legal structures using a combination of functionalist comparative law and systems analysis. The primary function of the Article 9 filing system is "to communicate the existence of filed financing statements to those who search the records."[178] To fulfill this function, Article 9 requires that a financing statement contain the name of the debtor, the name of the secured creditor, an indication of the collateral,[179] the mailing

173. Michaels, *supra* note 164, at 342.
174. *Id.*
175. *Id.*
176. Lynn M. LoPucki, *The Systems Approach to Law*, 82 CORNELL L. REV. 479, 481 (1997).
177. *Id.* (footnote omitted).
178. LoPucki, *supra* note 108, at 5.
179. These three pieces of information are required by U.C.C. § 9-502(a) in order for a financing statement to be effective. As a result, they are referred to by some "as 'the three holies' of the financing statement. Each must be given, and given cor-

address of the debtor and secured creditor, and an indication of whether the debtor is an individual or an organization.[180] A financing statement will lapse after five years unless a continuation statement is filed during the six-month window directly prior to the lapse date, and all records relating to a lapsed financing statement can be deleted from the system one year after lapse.[181] When a prospective creditor searches the filing statement for a pertinent financing statement, the creditor may only search an index, not the full text of the document, and the index only contains the debtor's name as it is contained in the financing statement on file.[182]

When a searcher obtains a financing statement, the "open drawer" concept of the filing system ensures that the searcher receives "absolutely everything related to the original financing statement (amendments, assignments, deletions, continuation statements, termination statements, etc.) . . . so that they have complete information as to the current status of the filed transaction."[183] Creditors filing financing statements make mistakes when entering the debtor's name on the form.[184] And even when the name was correct when initially listed, debtors change their names without informing their creditors, leaving the creditors vulnerable to an ineffective filing statement.[185] Filers also often unintentionally forget to file a continuance statement during the six-month continuation window.[186] Article 9 contains a system of complex and detailed rules for determining how to treat financing statements in each of these, and a variety of other, scenarios.[187] In other words, in order for the filing system to achieve its function, Arti-

---

rectly, for the financing statement to be sufficient." JAMES BROOK, PROBLEMS AND CASES ON SECURED TRANSACTIONS 145 (3d ed. 2016).

180. Although these pieces of information are not required for the financing statement to be effective, a financing officer is directed to reject a financing statement unless it contains the names of the debtor and secured creditor and these three additional items. *See* U.C.C. § 9-520(a), *reprinted in* CHOMSKY ET AL., *supra* note 107, at 885.

181. DOUGLAS J. WHALEY & STEPHEN M. MCJOHN, PROBLEMS AND MATERIALS ON SECURED TRANSACTIONS 112 (9th ed. 2014) (citing U.C.C. §§ 9-515, -522).

182. *See* U.C.C. § 9-519(c), *reprinted in* CHOMSKY ET AL., *supra* note 107, at 883; *see also* LOPUCKI ET AL., *supra* note 100, at 296 ("U.C.C. § 9-519(c) requires that the filing office index financing statements according to the name of the debtor.").

183. WHALEY & MCJOHN, *supra* note 181, at 113.

184. *See* LOPUCKI ET AL., *supra* note 100, at 298–303 (describing difficulties in identifying correct name for use in financing statements).

185. *Id.* at 394–96 (describing difficulty in maintaining an accurate financing statement through debtor name changes).

186. *Id.* at 388 ("Failure to file a necessary continuation statement timely is both a common error and a common source of legal malpractice claims.").

187. *See* U.C.C. §§ 9-338, -502, -503, -504, -506, -510, -515, -516, -518, -520 (AM. LAW INST. & UNIF. LAW COMM'N 2014); *see also* LOPUCKI ET AL., *supra* note 100, at 294–307, 311–21, 375–89, 393–404 (detailing the intricacies of applying these rules to common factual scenarios experienced by creditors).

cle 9 must supplement the filing system with legal rules intended to help mitigate the shortcomings of the system as it actually operates (in contrast to how it was intended to operate).

A primary function of DLT is providing a tamper-resistant, distributed, self-executing ledger of value transfers. Although the initial records recorded on DLT relate to monetary transfers, protocols have been built on top of those ledgers to offer a primary function of recording events other than monetary transfers. An example of such a protocol is that created by the Texas-based company Factom.[188] Factom designed a system of independent "censorship resistant blockchain[s] which [are] rendered immutable by the Bitcoin blockchain."[189] "Entries into the Factom Network are collected by federated nodes and protected against change using the Bitcoin hashpower."[190] In Factom, users can specify the rules for their chain, mandate that the initial entry in the chain hold a set of rules, and specify an enforced sequence to require the chain to automatically reject invalid entries.[191] Factom enables users to include whatever information in its chain entries that serves the purpose of the user.[192]

To create a crypto-legal structure that serves the function of the Article 9 filing system, the state filing office could create a Factom chain (or other similar DLT protocol) for use in recording financing statements. Each financing statement would represent an entry in the chain. The entries could continue to be indexed by name of the debtor so that a search would hit on all chain entries related to a particular debtor. The initial chain entry would specify the names of the debtor and secured party and indicate the collateral required for the financing statement to be effective, and an audit program could be constructed for validating this content. The enforced sequence would ensure that financing statements that do not contain the information required by U.C.C. § 9-520(a) are rejected. The enforced sequence would, therefore, serve the function of the filing officer in rejecting or

188. *See generally* Paul Snow et al., *Business Processes Secured by Immutable Audit Trails on the Blockchain*, FACTOM (Nov. 17, 2014), https://www.factom.com/devs/docs/guide/factom-white-paper-1-0 [https://perma.unl.edu/C2D4-AKFR].

189. *Factom Foundation*, FACTOM, https://www.factom.com/devs/factom-foundation [https://perma.unl.edu/WCP4-WJNX].

190. *Id.* A user of a Factom chain can write an unlimited number of entries into the system.

> The entries are organized into hierarchical sets of blocks. These blocks are then used to compute for a single hash every 10 minutes. We take these hashes and anchor them into other blockchains for redundant security. This design allows applications to write transactions faster, at a much lower cost, and with greater scalability than other blockchains. It also allows users to forgo dealing in tradable tokens.

Id.

191. Snow, et al., *supra* note 188.

192. *Id.*

accepting filings. The difference is that the enforced sequence would not, as is common at filing offices, incorrectly accept a filing that should be rejected for failure to comply. As a result, the rules regarding the partial effectiveness of wrongfully accepted filings could be eliminated.[193] Furthermore, compatible programming could be implanted into the initial chain entry to audit the chain for financing statements that are approaching the continuance window so that the secured party receives a reminder when a continuance statement should be filed.[194]

Doing so could simplify priority analysis and reduce litigation relating to unintentionally lapsed filings.[195] Every time a creditor filed an amendment or termination statement relating to an accepted financing statement, the chain would be updated accordingly; however, the prior history of the financing statement would not be lost and cannot be altered. The enforced sequence could incorporate an audit system that linked to the electronic databases of the Secretary of State's corporate records and state driver's-license records to monitor for changes in a debtor's name or location.[196] By eliminating the function of the Article 9 rules providing for grace periods to account for the difficulty in tracing name changes,[197] the crypto-legal structure would allow Article 9 to eliminate, or at least simplify, those rules as well. Amendments and new filings relating to transfers of collateral could be linked to corresponding entries in the chain, again allowing for simplification of the rules relating to grace periods for changes affecting information in the financing statement.[198] Finally, the ten-minute processing time would reduce the complexities of the existing system with regard to the "as of" filing dates when ordering searches,[199] and the ability of the chain to preserve the full history of the financing statement would achieve the current system's open-drawer policy.

Although a fully operational proposal for a crypto-legal structure that would modernize the Article 9 filing system would require much more detail, this summary demonstrates that, by capitalizing on features built into the DLT chosen to implement a crypto-legal structure (and this Article predicts that different DLT will work best for differ-

193. *See, e.g.*, U.C.C. §§ 9-516, -520, *reprinted in* CHOMSKY ET AL., *supra* note 107, at 878–80, 885–86.

194. I note here that Factom makes clear that this programming would need to be implemented client-side; that is, at the level of the filing office and not as a direct action by the chain.

195. LOPUCKI ET AL., *supra* note 100, at 375–89 (detailing the common problems engendered by the lapse system and providing examples of significant litigation).

196. I recognize that to do so would require negotiation of other applicable laws, such as those governing access to driver's-license records. However, the technological point that DLT makes doing so possible remains.

197. U.C.C. § 9-507, *reprinted in* CHOMSKY ET AL., *supra* note 107, at 866–67.

198. U.C.C. § 9-508, *reprinted in* CHOMSKY ET AL., *supra* note 107, 868–89.

199. LOPUCKI ET AL., *supra* note 100, at 297.

ent crypto-legal structures) and finding where those features serve the same functions as existing legal rules, substantive law can be simplified when creating the crypto-legal structure.[200] Arguably, the simplification also resolves many of the difficulties faced by the Article 9 system as a whole.[201]

2. Emergence of New Regulatory Actors

Even as the functional method enables simplification of substantive law implemented through crypto-legal structures, comparative scholarship on legal transplants instructs us to expect new legal elements and actors to emerge from transplanting law into DLT. In the process of creating crypto-legal structures, DLT is the foreign legal system, and the law to be implemented through DLT is the transplant. As "a central 'paradigm' in comparative law,"[202] the concept of legal transplants "investigates contacts of legal cultures and explores the complex patterns of change triggered by them."[203] The study of legal transplants led to an intense and extensive debate between two historically prominent comparative legal scholars, Alan Watson and Pierre Legrand, regarding whether legal transplants are possible, and if so, to what extent they are valuable.[204] Alan Watson argued that legal transplants are not only possible but have occurred throughout history, and opined that as a result, they are of utmost value to the comparative legal scholar.[205] Pierre Legrand, on the other hand, argued just as forcefully that legal transplants do not exist, and as a result, there is little value for the comparative legal scholar in pursuing the study of such imaginary concepts.[206] In the gap between these two extreme positions, comparative legal scholars have developed a substantial body of literature devoted to the study of why, with what effect, and how legal transplants take place.

The comparative study of legal transplants has identified several reasons for why legal transplants are undertaken, including technological change.[207] With regard to the effect of legal transplants, many

200. Note that, as a result, this specific crypto-legal structure might be best built for and recommended by the American Law Institute and the Uniform Law Commission, and then recommended to the states as part of the uniform-law process.
201. For an in-depth assessment of those difficulties, see LoPucki, *supra* note 108.
202. Michele Graziadei, *Comparative Law as the Study of Transplants and Receptions*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW, *supra* note 161, at 441, 443.
203. *Id.* at 442.
204. Jacques du Plessis, *Comparative Law and the Study of Mixed Legal Systems*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW, , *supra* note 161, at 477, 487–89.
205. ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW 21–30 (2d ed. 1993).
206. Pierre Legrand, *The Impossibility of "Legal Transplants"*, 42 MAASTRICHT J. EUR. & COMP. L. 111 (1997).
207. Graziadei, *supra* note 202, at 455. Other identified reasons include migration of a population, religious influence, imposition following military conquest, imitation

comparative legal scholars recognize that "when those vested with authority have decided what law to import, the process of adaptation to the local environment will often add new and unexpected elements to the import."[208] Thus, a transplant should not be expected to work exactly the same way when implemented through computer code as when implemented in writing, by a regulator, or by a judge.[209] As Watson explained, "[a] successful legal transplant—like that of a human organ—will grow in its new body and become part of that body just as the rule or institution would have continued to develop in its parent system. Subsequent development in the host system should not be confused with rejection."[210] Gunther Teubner explained it another way, saying the term legal transplant "creates the wrong impression that after a difficult surgical operation the transferred material will remain identical with itself playing its old role in the new organism."[211] Because some legal institutions are so intricately intertwined

---

because of the perceived prestige of a legal paradigm, and transplants undertaken at the behest of international economic institutions. *Id.* at 456–61.

208. *Id.* at 465; *see also* WERNER MENSKI, COMPARATIVE LAW IN A GLOBAL CONTEXT 51 (2d ed. 2006) ("[R]eceived laws have everywhere been adapted to suit local conditions, and transplants everywhere manifest themselves as new hybrids." (footnote omitted)); Günter Frankenberg, *Constitutional Transfer: The IKEA Theory Revisited*, 8 INT'L J. CONST. L. 563 (2010) (discussing this idea as "recontextualization"); Graziadei, *supra* note 202, at 465 ("[T]he process of adaptation to the local environment will often add new and unexpected elements to the import. This is inevitable. It makes little sense to view these additions as distortions of the original model that would inexplicably fail to be reproduced locally."); Ralf Michaels, *"One Size Can Fit All"—On the Mass Production of Legal Transplants*, *in* ORDER FROM TRANSFER: STUDIES IN COMPARATIVE (CONSTITUTIONAL) LAW 18 (Gutner Frankeberg ed., 2013) ("People take Ikea furniture and assemble it differently from the producer's intention. And then they share their new constructions on the internet and can thus inspire other users. Such creative reuse may not be favored by IKEA—just as the creative re-use of legal rules in a recipient country may not be what the donor country intended. But it may well serve the needs in the recipient country." (footnote omitted)); Gunther Teubner, *Legal Irritants: Good Faith in British Law or How Unifying Law Ends Up in New Divergences*, 61 MOD. L. REV. 11, 12 (1998) (arguing that transplants must be understood instead as "legal irritants," "which triggers a whole series of new and unexpected events").

209. Frank Upham, *Mythmaking in the Rule-of-Law Orthodoxy*, *in* PROMOTING THE RULE OF LAW ABROAD 75, 100 (Thomas Carothers ed., 2006) ("Although it is highly unlikely that the transplanted system will operate as it did in its country of origin or as intended by the borrowing country, it does not follow that it will have no social effect." (footnote omitted)).

210. WATSON, *supra* note 205, at 27. Recent scholarship, even while arguing that a one-size-fits-all approach can work, nevertheless agrees with this understanding of legal transplants. *See* Michaels, *supra* note 207, 17 ("It is true, as critics of transplants have pointed out, that legal rules will often acquire a different meaning in the recipient country than they do in the donor country. An attempt to replicate the meaning and effects from the donor country in the recipient country is thus doomed to fail.").

211. Teubner, *supra* note 208, at 12.

with social norms, a transplant will not only cause a legal change but will also trigger changes in the related social system.[212] The social change will then cause the society to revisit the form of the transplanted legal institution, creating a cycle of change.[213] As a result, comparative law expects the transplant to change and grow until the institution resembles an organic part of the importing society.

Considering the nature of DLT and smart contracts, the emergence of crypto-legal structures will introduce new regulatory actors into the legal sphere: certain self-executing elements of the code and the developers that translate the law into code. Administrative law and administrative practice dictate the interaction between the governed and the regulators that govern.[214] Taken together, administrative law and administrative practice form a system in which "congress regulates by delegating to intermediaries whose behavior is shaped by the rules and practices governing administrative decisionmaking."[215] In this context, the regulatory process is shaped by ever-changing combinations of administrative law, administrative behavior ("the informal norms that inform regulatory decisions"), oversight by the other branches of government, and each agency's "organizational structure and culture."[216]

The introduction of crypto-legal structures will disrupt these elements of the regulatory system as it is presently known and understood in at least two ways. First, because the smart-contracting features of DLT that will make many of the crypto-legal structures possible are self-executing, those features arguably become new regulatory agents. In the computer-science discipline that created DLT, the term "agent" includes "a piece of software that acts on behalf of its user and tries to meet certain objectives or complete tasks without any direct input or direct supervision from its user,"[217] and "computational systems that inhabit some complex dynamic environment, sense and act autonomously in this environment, and by doing so real-

212. *Id.* at 28.

213. *Id.*

214. Steven P. Croley, *Theories of Regulation: Incorporating the Administrative Process*, 98 COLUM. L. REV. 1, 6 & n.8 (1998) ("'Administrative law' refers simply to the legal-formal rules and doctrines governing the relationship between regulators and private parties—the 'law on the books.' 'Administrative practice' refers to the operation of those rules in actual administrative decisionmaking processes—focusing on who, when, and how parties participate in those processes.").

215. *Id.* at 26–27.

216. *Id.* at 28.

217. SAMIR CHOPRA & LAURENCE F. WHITE, A LEGAL THEORY FOR AUTONOMOUS ARTIFICIAL AGENTS 6 (2011) (quoting JOHN J. BORKING, B.M.A. VAN ECK & P. SIEPEL, INTELLIGENT SOFTWARE AGENTS: TURNING PRIVACY THREAT INTO A PRIVACY PROTECTOR (1999)).

ize a set of goals or tasks for which they are designed."[218] Under such a conception, computer code can take on its own autonomous agency. In the context of cryptolaw, this might take the form of a crypto-legal structure composed of smart contracts with embedded elements of predictive technology and machine-learning algorithms. In such a case, the crypto-legal structure could be driven by a crypto-regulatory agent—computer code that

> possess[es] a goal-directed nature: a final result may be specified and [code], given knowledge of the actions required to accomplish a task, can autonomously decide how to carry out the task given its resources and the features of the environment; it can select among the various choices available to it along several dimensions of preference.[219]

In other words, cryptolaw would enable a world of microdirectives[220] in which, instead of delivering a microdirective or range of microdirectives to an individual for choice of compliance, a range of microdirectives is derived, a choice is made, and the choice is executed, all by the crypto-regulatory agent that exists within the crypto-legal structure.[221] Such crypto-regulatory agents would arguably qualify as legal agents of their human regulator principals.[222] Although such a suggestion may sound radical upon first read, some

---

218. *Id.* (quoting Pattie Maes, *Artificial Life Meets Entertainment: Lifelike Autonomous Agents*, 38 COMM. ACM 108, 108–14 (1995)).

219. *Id.* at 9.

220. Casey & Niblett, *supra* note 16, at 1–3 (describing a microdirective as an easy-to-follow behavioral directive for legal compliance created by technology). Casey and Niblett explain that microdirectives will be created through the following process:

> First, they will take a standard-like policy objective, analyze its application in all possible contexts, and create a vast catalog of legal rules—each of which is tailored to best achieve the objective in a specific scenario. Second, when a regulated actor is in any actual scenario, the technologies will search the vast catalog and identify the specific rules that are applicable. Third, they will translate those rules into a simple microdirective on how the regulated actor can comply with the law. Fourth, they will communicate that micro-directive to the regulated actor in a timely and efficient manner.

Id. at 12.

221. This is made possible, in part, by the smart-contracting features of DLT, which, when combined with predictive technology and machine-learning capacity, enable autonomous execution of the program. DLT can be imbued with

> the ability to operate without the direct intervention of humans or other agents, and to exert nonsupervised control over its own actions and internal states; the social ability or capacity to interact with other artificial agents or with human beings; the proactive ability to initiate goal-directed behavior; the reactive ability to perceive an environment and respond to changes within it; the ability to adjust to the habits, working methods, and preferences of users, other agents, or humans; the ability to move around a virtual or physical environment; and representativeness, or the attribute of being a representative of, or intermediary for, another agent or person.

CHOPRA & WHITE, *supra* note 217, at 10 (footnote omitted).

222. *Id.* at 23.

case law takes this very approach and views computer systems as the legal agents of the corporate entities that employ them.[223] Alternatively, such crypto-regulatory agents may be viewed as possessing their own legal personhood, in light of the fact that "[t]hey take actions that they initiate, and their actions can be understood as originating in their own reasons."[224] In either case, the choices made by the crypto-regulatory agent will not always be the expected choice.[225] What remedies will belong to the governed when the computer code makes an unexpected or undesirable decision, or both? Who will be at fault if the code executes prematurely because it misread the circumstances? Who will be penalized when compliance efforts are compromised because the designated crypto-regulatory agent took an unpredictable turn? These and other similar new questions of substantive law will emerge along with the rise of these new regulatory agents, disrupting the present understanding and theory underpinning substantive areas of law such as that governing the administrative process.

A second regulatory actor will emerge as well—the developers that code the law and create the crypto-legal structures and the crypto-regulatory agents that execute them. Lessig argued that coders were already playing this role in the early days of the Internet. "As the world is now," Lessig wrote in 1999, "code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed."[226] His discussion of that phenomenon arguably made the case for coders exer-

223. United States v. Flowerday, 28 M.J. 705, 707–09 (A.F.C.M.R. 1989); Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473–74 (Cal. Ct. App. 1996).

224. CHOPRA & WHITE, *supra* note 217, at 189. *But see* Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 2012 STAN. TECH. L. REV. 5, 21 ("The law as it is currently configured cannot vest ownership of the copyright in a procedurally generated work in the work's author-in-fact because the work's author-in-fact—a generative software program—has no legal personhood." (footnote omitted)); Ralph D. Clifford, *Intellectual Property in the Era of the Creative Computer Program: Will the True Creator Please Stand Up?*, 71 TUL. L. REV. 1675, 1696–97 (1997) (looking at patent law and the requirement of a human inventor). Notably, these authors examine laws which would offer legal privileges to the computer program, whereas when the program is acting as a regulatory actor, the law would seek to place responsibility on the computer program. Whether that distinction matters for the purposes of determining whether and when to extend legal personhood to certain autonomous, creative computer software, or both, deserves further attention, but that is beyond the scope of this Article.

225. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 540 (2015) ("The prospect of useful but unexpected problem solving by machines presents a number of challenges for the law.").

226. LAWS OF CYBERSPACE I, *supra* note 155, at 60.

cising soft power.[227] Just as crypto-legal structures can be conceived of as an extreme form of code as law, so too can the role of the coders in creating these structures be seen as playing an enhanced regulatory role in comparison to the role Lessig described. In cryptolaw, coders would no longer exert soft regulatory power by merely developing the norms that shape DLT. Instead, the coders step into the role of actual regulators, exerting the regulatory coercive powers of the state.

This new, enhanced role of coders will lead to new issues for adjudication, especially considering the changes to enforcement structures predicted in Part III.B. below. When a crypto-regulatory agent goes rogue, can the governed pursue remedies against the developer that created it? What if the code was flawed from the beginning; would the developer be subject to a product liability claim for failure to code a law properly?

Further, extensive research evidences the extent to which developers frequently write implicit biases into the code and algorithms they create.[228] For example, research demonstrates that although credit scores are held out as impartial predictors of credit worthiness, the scores are generated by algorithms that engrain bias into the system rather than eliminate it.[229] "Credit scores" they explain,

> are only as free from bias as the software and data behind them. Software engineers construct the data sets mined by scoring systems; they define the parameters of data-mining analysis; they create the clusters, links, and decision trees applied; they generate the predictive models applied. The biases and values of system developers and software programmers are embedded into each and every stage of development.[230]

These concerns are compounded by the inherent risk that technological automation of legal processes may erode procedural safeguards for individual rights.[231] For example, "[s]ome systems adjudicate in secret, while others lack recordkeeping audit trails, making review of the law and facts supporting a system's decisions impossible."[232]

As cryptolaw begins to take shape, processes for rooting out such bias and increasing protections for individual rights could be developed to prevent similar outcomes from infecting crypto-legal structures by choosing the mix of DLT services best suited for that purpose.

---

227. *Id.* Lessig argued that the code writers influenced norms that regulate behavior because "[t]hey are the ones who set [the Internet's] nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is." *Id.*
228. FRANK PASQUALE, THE BLACK BOX SOCIETY 110–13 (2015).
229. Citron & Pasquale, *supra* note 17, at 13.
230. *Id.* at 13–14 (footnotes omitted).
231. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1253 (2008) ("Computer programs seamlessly combine rulemaking and individual adjudications without the critical procedural protections owed either of them. Automation generates unforeseen problems for the adjudication of important individual rights." (footnote omitted)).
232. *Id.* (footnote omitted).

If certain bias creeps into crypto-legal structures anyway, what remedies will be available to those governed by them? Will the developer be subject to suit? Will the regulatory body that hired the developer be the proper target for suit? Further, if the developers code the crypto-regulatory agents and those agents choose among microdirectives for the governed in a self-executing enforcement of certain laws, will that not signal a subtle shift away from adjudication as an activity of the judicial branch and towards placing the power of adjudication, in real time, in the hands of regulatory agencies led by one or both of the other branches of government? How often, and to what degree, will that adjudication be influenced by the hidden bias of the software developer?

Although for some these questions might invite a prediction of the death of adjudication,[233] I predict instead, by following the comparative insights from functional equivalence and legal transplants to their logical conclusion, that the emergence of cryptolaw will simply lead to new adjudicators, forms of adjudication, and issues for adjudication. We might imagine a subtle shift in the issues adjudicated by judges, with the more mundane issues decided by smart-contracting crypto-legal structures and the crypto-legal agents that make them run, while the new, more daunting issues of who to hold accountable for bugs in crypto-legal structures, when bugs have occurred and when such bugs have caused damage to individuals, will be pushed to the top of the judicial docket. We might imagine that such a dual-tiered system of adjudication could be conceived of as "crypto-adjudication."[234]

Over time, then, an aggregation of interacting crypto-legal structures with varying levels of autonomy will result in the simplification and reconfiguration of substantive law and reconstitute the makeup of legal actors in the administrative process. These changes will impact the legal system beyond the substance of law because, ultimately, substantive law is connected to the structure of institutions through which regulatory action unfolds.[235] Consequently, these subtle shifts in substantive law will lead to more seismic shifts in the foundations of the legal system—in the legal structures that make up the system.

B. Disruption of Legal Structure

The term "legal structure" refers to a legal system's "skeletal framework; it is the permanent shape, the institutional body of the system, the tough rigid bones that keep the process flowing within

233. *See, e.g.*, Casey & Niblett, *supra* note 16, at 39 ("The proliferation of clear micro-directives largely obviates the need for ex post adjudication.").

234. Admittedly, such issues deserve their own thorough examination, and I therefore acknowledge here that they exist but reserve further comment for later work.

235. Croley, *supra* note 214, at 27.

bounds."[236] Essentially, each "[s]tructure becomes . . . custom or habit" such that "social meanings clump about each structure," giving them "social-psychological and cultural boundaries."[237] As a result, "[s]tructures are patterns of behavior that persist over time—vessels or containers that the culture slowly welds into shapes."[238] Cryptolaw can be conceptualized as disruptive discourse regarding existing legal structures in at least two important ways. First, the emergence of crypto-legal structures in societies that rely heavily on common law adjudication will disrupt established patterns of legal enforcement. Second, the emergence of crypto-legal structures will disrupt the policy considerations that inform lawmakers' choices when constructing laws, disrupting established forms of law. Ultimately, the cryptolaw discourse may disrupt the way that the governed interact with the law as the governed attach new social meanings to the new crypto-legal structures that emerge.

1. Disruption of Established Patterns of Enforcement and Related Regulatory Policy Choices

At the broadest level, legal structures are tied to legal traditions,[239] meaning that a legal system's roots in the English common law or the French civil law stem from that system's unique historical and political context, and thereby significantly impact the shape of the

236. FRIEDMAN, 1975, *supra* note 159, at 14.

237. *Id.* at 158.

238. *Id.* at 162.

239. I recognize that there is a debate in the literature regarding the extent to which the difference in legal structures roughly corresponds to a difference in legal traditions (or legal origins, depending upon whether your primary discipline is law and economics or comparative law). *See, e.g.*, Holger Spamann, *Contemporary Legal Transplants: Legal Families and the Diffusion of (Corporate) Law*, 2009 BYU L. REV. 1813, 1813–14 ("Contemporary knowledge on comparative legal systems is strangely bifurcated. On the one hand, some of the most sophisticated comparative lawyers assert that there are few if any relevant differences between common and civil law today, judging by key characteristics of the legal system, such as case law versus statutory law, the systemization of the law, or the lasting influence of Roman law, which are the traditional markers of the common/civil law distinction. On the other hand, a very influential literature in economics—known as the 'legal origins literature'—claims that empirically, the substantive rules in areas of economic policy ranging from investor protection to military conscription differ systematically between common and civil law countries." (footnotes omitted)). That debate is beyond the scope of this Article. I mention it here only to recognize its prevalence and to note that if cryptolaw disrupts legal structures in the ways predicted throughout this Article, the debate may be rendered moot as the underlying premises upon which it is based may transform altogether as crypto-legal structures replace many of the structures we take for granted at present. While this point may be worthy of its own detailed treatment, I make it here in passing to drive home the idea that the potential disruptive effect of cryptolaw on law as we know it runs vast and deep.

legal structures within the system.[240] Both systems employ the legal structure of codes of laws.[241] In the common law system, such codes and statutes are expected to interact dynamically with judge-made law, giving practitioners and judges "some flexibility to disregard [code] provisions when they conflict with the basic principles of common law."[242] Common law systems view the common law itself as a legal structure, considering it to be the "legal repository of the moral values of the people."[243] On the other hand, in civil law jurisdictions, judges are expected to exercise deference to the provisions of the code, which makes codes arguably much more powerful in civil law jurisdictions than common law jurisdictions.[244] The emergence of cryptolaw has the potential to disrupt this fundamental difference between legal structures. By translating statutes and regulations into cryptographic, smart-contracting computer code to create crypto-legal structures, the gap between the importance of codes in common and civil law jurisdictions will narrow.[245] Crypto-legal structures will self-execute, and enforcement will occur in real time,[246] reducing flexibility to later argue before a judge that any violation was a result of complying with overruling principles of common law.

The implication for the common law system in the United States is that by disrupting established patterns of enforcement, cryptolaw will also disrupt the practical aspects of and theoretical justifications for legislation and its implementing regulations. Legislation and implementing regulations are legal structures because they are unquestionably patterns of behavior that have persisted over time in industrialized nations.[247] Scholars have argued for decades about the

240. *See generally* Andrei Shleifer & Edward L. Glaeser, *Legal Origins*, *in* THE FAILURE OF JUDGES AND THE RISE OF REGULATORS 209 (Andrei Shleifer ed., 2012).

241. *Id.* at 226.

242. *Id.*

243. DAVID DYZENHAUS, RECRAFTING THE RULE OF LAW 3 (1999). Dyzenhaus also describes the common law as "value-laden background against which legislation is be interpreted," making it clear that the common law itself fits within Friedman's conception of a legal structure. *Id.*

244. Shleifer & Glaeser, *supra* note 240, at 226.

245. Or, arguably, depending on your position in the debate on the degree of difference between legal traditions, the gap will narrow further.

246. There is a debate in the literature regarding whether it is advisable to make noncompliance with laws impossible through technology. *See, e.g.*, Michael L. Rich, *Should We Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y 795 (2013). This Article does not engage that debate but acknowledges, particularly in Part III, that the issues raised in that debate are both important and applicable to the emergence of cryptolaw and the implication of cryptolaw on the legal system.

247. Andrei Shleifer, *The Enforcement Theory of Regulation*, *in* THE FAILURE OF JUDGES AND THE RISE OF REGULATORS, *supra* note 240, at 1, 1 ("Government regulation is extensive in all rich and middle-income countries. . . . There is surely a lot of variation across countries, but it pales by comparison with the raw fact of ubiquity.").

social-psychological and cultural boundaries that push societies to choose regulation over other legal structures.[248] One prominent theory regarding the social meaning clumped around regulatory artifices is that regulation is a less expensive, more predictable, less biased alternative to enforcing legal rules than court-based adjudication.[249] In this conception of regulation, it does not matter whether regulation is in the form of government ownership of a market, rules for required precautions that impose penalties for compliance failures, or rules left to private enforcement. Rather, what matters is that the public trusts a regulated world because regulation is thought to reduce costs of business by more precisely defining the requisites for liability.[250] Others argue that regulators undertake decisions after considering alternatives in the context of a regulatory economy governed by supply-and-demand-based exchanges of regulatory goods.[251] In this public-choice theory, regulatory decisions result from the meeting of private economic demands by political supply from the public sector.[252] Another group of scholars argues that regulatory outcomes reflect the relative investment of various groups in obtaining public goods to further their interests.[253] A variety of other explanations for regulatory outcomes compete with those mentioned here.[254]

Technology both challenges these theories[255] and offers new ways to make the policy choices that lead to regulatory outcomes. For example, law-and-technology scholars have argued that technology can, and perhaps should, disrupt the basis for lawmaking for some time. Some argue that technological advances in harvesting and marshalling data enables real-time feedback to regulators for use in a dynamic model of regulation that allows more rapid response to market

248. *See generally* Croley, *supra* note 214; George L. Priest, *The Origins of Utility Regulation and the "Theories of Regulation" Debate*, 36 J.L. & ECON. 289 (1993).

249. Shleifer, *supra* note 247, at 15.

250. *Id.* at 17.

251. Croley, *supra* note 214, at 34 (citing George J. Stigler, *The Theory of Economic Regulation*, 2 BELL J. ECON. & MGMT. SCI. 3 (1971)).

252. *Id.* at 35.

253. *Id.* at 57 (citing Gary S. Becker, *A Theory of Competition Among Pressure Groups for Political Influence*, 98 Q.J. ECON. 371 (1983)) (describing the "neopluralist theory" of regulation by Gary Becker).

254. A full catalogue of these theories is beyond the scope of this Article, but they include the public-interest theory, the civic-republican theory, *see* Croley, *supra* note 214, at 65–85, and the capture theory, *see* Richard A. Posner, *Theories of Economic Regulation*, 5 BELL J. ECON. & MGMT. SCI. 335 (1974).

255. Kaal & Vermeulen, *supra* note 15, at 5 ("The ex-post facts-based and trial-and-error-rulemaking with stable and presumptively optimal rules in the existing regulatory framework often produces suboptimal regulatory outcomes that are no longer sustainable in an environment of exponential disruptive innovation." (footnotes omitted)); *see* Wulf. A. Kaal, *Dynamic Regulation of the Financial Services Industry*, 48 WAKE FOREST L. REV. 791 (2013).

changes.[256] Additionally, the "RegTech" phenomena in the context of the BSA Regulations provides evidence that the market also hopes to push regulation toward a more technology-driven, rapidly responsive regulatory environment. RegTech, shorthand for regulatory technology, offers BSA-covered financial institutions automated systems for complying with the detailed reporting required by the BSA Regulations.[257] The financial and FinTech industries encourage regulators to further adapt RegTech compliance solutions through tailored drafting and enforcing of the BSA Regulations and related compliance obligations.[258] The emergence of crypto-legal structures will allow industry further opportunity to bring order, predictability, and efficiency to compliance efforts while disrupting the theories of regulation and the legal structures that they seek to explain. Specifically, cryptolaw will bring theories of data-driven dynamic regulation, endogenous regulation, and the RegTech phenomena to their logical conclusions. RegTech would no longer be limited to technology that assists covered institutions in meeting their compliance obligations more efficiently, but rather, the technology would be the regulation. A firm that adopts the prescribed crypto-legal structure would be prima facie compliant and would maintain a designation of compliance so long as its systems passed regular audits. Audits could be conducted efficiently and at regular intervals, with variances prescribed for rogue actors. Firms that failed audits would become natural targets for enforcement. Further, the public would be more readily able to ascertain which companies are compliant and worthy of trust and which companies should be avoided. In other words, the regulators could bake the regulatory theory into the code, making regulatory objectives more transparent to the industry subject to them and offering public benchmarks for assessing which entities are responsible corporate citizens.

This added element of transparency for both the regulator and the regulated will alter the theories of regulation debate, adding new the-

256. Kaal & Vermeluen, *supra* note 15, at 4 ("We show that data derived from venture capital investments can function as a dynamic regulatory supplement that can help address the legal challenges presented by disruptive innovation. Venture capital's financial allocations to innovative projects can provide feedback for dynamic regulation of disruptive innovation.").

257. Elzio Barreto, *Financial Firms Seek RegTech to Cut Regulatory Chores, Fight Crime*, REUTERS (Nov. 11, 2016), http://www.reuters.com/article/us-asia-fintech-regulations-idUSKBN1360UQ [https://perma.unl.edu/7ZPJ-RT79].

258. Kevin Petrasic, Benjamin Saul & Helen Lee, *RegTech Rising: Automating Regulation for Financial Institutions*, WHITE & CASE (Sept. 26, 2016), http://www.whitecase.com/publications/insight/regtech-rising-automating-regulation-financial-institutions [https://perma.unl.edu/6CUA-EFFF] ("A growing number of companies and regulators use regtech solutions to increase the efficiency and effectiveness of compliance while reducing costs. Regtech may also prove essential to regulating emerging fintech applications that are difficult to monitor or manage under legacy regimes.").

ories and making certain existing theories more relevant. In other words, cryptolaw offers a disruptive new way to think about the justifications for and purposes of regulation and enforcement even more so than current law-and-technology literature expects that big-data, RegTech, predictive, and other technology will. Most immediately, cryptolaw presents an opportunity to consider new theories of regulatory process, and, in the long term, thereby endogenously give rise to new ways of thinking about regulatory origin.

2. Disruption of Choices in Legal Forms

Because cryptolaw offers disruptive new models for regulatory process, origin, decision-making, and enforcement, cryptolaw should also be expected to disrupt the structural choices of lawmakers as they enact laws. The most obvious area for such disruption is in the lawmakers' choice between rules and standards. The premise that technology will disrupt the choice between enacting law in the form of rules or standards is not new. Anthony Casey and Anthony Niblett argue that advances in predictive and communication technology will enable a system that "identif[ies] the rules applicable to an actual situation and inform[s] the regulated actor exactly how to comply with the law."[259] As a result, they argue that these "micro-directives will become the dominant form of law, culminating in the death of rules and standards."[260] Casey and Niblett predict that although the legislature may view its role as creating laws that continue to look like standards, the regulated individual will only see a "simple and easy-to-follow directive."[261] Notably, a microdirective leaves the regulated individual a choice of whether to comply with the instruction or not.[262] Although Casey and Niblett argue that this will lead to a reduced role for judges, it may also lead to new questions for adjudication. For example, what claim would an individual have if he or she follows the microdirective to his or her detriment? What happens if the underlying algorithm leading to the microdirective is flawed? When does an individual have a defense for ignoring a microdirective given the circumstances facing the individual?

Crypto-legal structures will further alter the way in which the regulated individual receives and interacts with the law. Conceived of as an extreme form of code as law, crypto-legal structures present a mechanism for covered entities to efficiently comply with regulations and to ensure that their customers undertake compliant transactions. In the BSA Regulations context, for example, the financial institution

259. Casey & Niblett, *supra* note 16, at 3.
260. *Id.*
261. *Id.* at 4.
262. Casey & Niblett, *Self-Driving Laws*, *supra* note 22, at 439 ("Upon receiving the micro-directive, the individuals may still elect to violate the law.").

must choose whether to be prima facie compliant or not. FinCEN could keep a list of those covered institutions that adopt compliant crypto-legal structures and are therefore at low risk of allowing money-laundering activity or suspicious transactions. In turn, individual consumers would be presented with a choice: bank with an institution that the world knows to be compliant or bank with an institution that essentially operates in the shadows. The result is that once the initial compliance choice is made, the self-executing code of the crypto-legal structure ensures that compliance trickles down to all actors in the institution, including individual consumers. The change to legal structures would be significant. The effect would be that the choice of whether to comply with a legal rule would no longer be limited to individual transactions but rather to patterns of behavior overall.

As Casey and Niblett acknowledge, "the move from micro-directives to automatic restraint and strict coercion is enormous."[263] Crypto-legal structures represent a vehicle for the move from microdirectives to automatic restraint. Where the microdirective appears to the regulated individual as an easy-to-follow instruction, crypto-legal structures would not appear so vividly, but rather, they would become embedded in the fabric of society. An individual's choice would be limited to whether to participate in the law-abiding society or not, and individual choices on more discrete issues would be narrowed from within the system of operation accordingly. Although this may raise considerations of individual autonomy that cause alarm,[264] it also offers some benefit. Specifically, the interwoven nature of regulation would allow for greater endogenous feedback loops to enable regulation to more closely reflect economic and social realities. As Lessig once conceptualized it in the context of the Internet, "[w]e can build, or architect, or code [crypto-legal structures] to protect values that we believe are fundamental, or we can build, or architect, or code [crypto-legal structures] to allow those values to disappear."[265] The decisions about how to balance these competing interests will reshape choices in legal forms, ultimately reshaping the way lawmakers think about the law they make, not just in terms of rules and standards but also in the appropriate mix of ex ante regulation and ex post facto punishment.[266] Such fundamental changes will culminate in a significant disruption of legal culture.

C. Disruption of Legal Culture

Conceptualizing cryptolaw as disruptive legal discourse highlights the significant impact that crypto-legal structures will make on the

263. *Id.* at 440.
264. Indeed, such issues should be considered at length in future work.
265. LAWS OF CYBERSPACE I, *supra* note 155, at 6.
266. See my initial consideration of this issue in Reyes, *supra* note 19.

understanding, study, and significance of legal cultures and legal traditions, and their role in shaping real-life interactions with the law. Varying definitions of the concept of legal culture exist. Comparative legal scholars consider that "[l]egal culture often describes merely an extended understanding of law and is thus synonymous with 'living law' (*Eugen Ehrilch*) or 'law in action' (*Roscoe Pound*)."[267] Law-and-sociology scholars view legal culture "as the values, ideas and attitudes that a society has with respect to its law (*Lawrence M. Friedman, James Q. Whitman*)."[268] Friedman viewed legal culture as the "attitudes, values, and opinions held in society, with regard to law, the legal system, and its various parts."[269] According to Friedman, "[I]t is the legal culture which determines when, why, and where people use law, legal institutions, or legal process; and when they use other institutions, or do nothing."[270] In this vein, the law as lawyers understand it may vary by community because a "shared mental model" of law in such communities "implicitly proclaims 'this is how we do things'" and therefore, legal culture serves as "primary law," while the law on the books acts as "merely background with which the model interacts."[271] In other words:

> [T]he term "legal cultures" . . . stands for an operative and creative contribution, through social activity rooted in underlying social culture, to express how people experience legal phenomenon, conceived as a kind of objectified poten-

267. Ralf Michaels, *Legal Culture, in* OXFORD HANDBOOK OF EUROPEAN PRIVATE LAW (Basedow, Hopt & Zimmermann eds., forthcoming) (on file with author).

268. *Id.*

269. FRIEDMAN, 1977, *supra* note 159, at 76. As Professor Michaels indicates, many variations on the definition of legal culture, to the extent scholars bother to use an explicit definition when wielding the term, exist. Michaels, *supra* note 267. Other such definitions include the following: "A specific way in which values, practices and concepts are integrated into the operation of legal institutions and the interpretation of legal texts." Mark Van Hoecke & Mark Warrington, *Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative Law*, 47 INT'L & COMP. L.Q. 495 (1998) (internal quotations and citation omitted). A further variation is as follows: "'[C]ulture' concerns frameworks of intangibles within which interpretive communities operate and which have normative force for these communities. . . . Because rules are but the outward manifestation of an implicit structure of attitude and reference, they are a reflection of a given legal culture." Pierre Legrand, *European Legal Systems Are Not Converging*, 45 INT'L & COMP. L.Q. 52, 56–57 (1996).

270. FRIEDMAN, 1977, *supra* note 159, at 76. According to Friedman, legal culture exudes "lines of force, pressures, and demands that envelop legal institutions and ultimately determine their shape." LAWRENCE M. FRIEDMAN, THE REPUBLIC OF CHOICE: LAW, AUTHORITY, AND CULTURE 4 (1990) [hereinafter FRIEDMAN, 1990].

271. Lynn M. LoPucki, *Legal Culture, Legal Strategy, and the Law in Lawyers' Heads*, 90 NW. U. L. REV. 1498, 1501 (1996). Friedman would refer to the law in lawyers' heads that LoPucki describes as "internal legal culture"—the attitudes and values of professionals that work within the legal system. FRIEDMAN, 1977, *supra* note 159, at 76; FRIEDMAN, 1990, *supra* note 270, at 4. External legal culture would be the attitudes and values towards law of the general public. *See* FRIEDMAN, 1990, *supra* note 270, at 4.

> tiality, how and into what they form it through their co-operation, how and in what way they conceptuali[z]e it, and in what spirit, frame and purpose they make it the subject of theoretical representation and operation.[272]

If we currently conceptualize legal culture as a societal force that transforms the law on the books (black-letter law) into the law in action (law as it is experienced by the governed), how will cryptolaw conceptualize legal culture in the context of crypto-legal structures? There are arguably at least two possible lines of impact. First, crypto-legal structures could so narrow the gap between the black-letter law and the law in action that legal culture evaporates as both a concept and as an agent of legal change. Second, if the black-letter law is the law as it is written by legislatures and crypto-legal structures are self-executing, we might conceive crypto-legal structures as law in action, suggesting that the locus of legal culture will shift from professionals in the field to the developers that code crypto-legal structures.

1. Cryptolaw Envisions a World Without Law Lag

The legal culture prevailing in the current regulatory system depends upon consensus and assumes value in the "long, drawn-out feedback process that involves hearings, proposed rules, the submission of comment letters, and finally agency lawyers finalizing a rule after considering the comments."[273] Product development, on the other hand, happens very quickly.[274] The result is that "[n]ew regulations pertaining to an innovative product could be obsolete before they are finalized."[275] In fact, "[t]he growing number of rule enactments, revisions, and revocations suggests that existing rules and institutional structures for rulemaking are becoming less capable of addressing the rapid pace of change."[276]

This conception of law lag[277] applies the law on the books compared to the law-in-action concept from the study of legal culture to the field of law and technology. Implementing the law on the books through DLT will enable real-time feedback that could narrow or eliminate law lag. Essentially, the crypto-legal structure will be the law in action. When product development in the industry is no longer com-

272. Csaba Varga, *Legal Traditions? In Search for Families and Cultures of Law*, 46 ACTA JURIDICA HUNGARICA 177, 182 (2005).
273. Kaal & Vermeulen, *supra* note 15, at 19–20.
274. *Id.* at 20 (emphasis omitted).
275. *Id.* (citing Jo Ann S. Barefoot, *Disrupting FinTech Law*, FINTECH L. REP., Mar.–Apr. 2015, at 10).
276. Wulf A. Kaal, *Evolution of Law: Dynamic Regulation in a New Institutional Economics Framework*, *in* FESTSCHRIFT ZU EHREN VON CHRISTIAN KIRCHNER 1211, 1212 (Wulf A. Kaal, Matthias Schmidt & Andreas Schwartze eds., 2013).
277. Priest, *supra* note 248, at 302 (describing the difficulties of various regulatory models in "adapting . . . over time to new conditions, and monitoring compliance . . . for the benefit of the citizenry").

patible with current crypto-legal structures, compliant industry actors would approach regulators with the technical mismatch, and the software developers that initially coded the crypto-legal structure would work with industry to adjust the code implementation to uphold the law while also enabling industry to maintain compliance even while innovating. In other words, computer code can be adapted more quickly to changing technology than natural-language statutes interpreted by regulatory agencies struggling to keep pace with technological changes. If crypto-legal structures can be continually adapted by the software developers that code them in order to adjust to changing industry uses of technology, the concept of a separate legal culture that helps shape the law as it is carried out in society may diminish or evaporate altogether. The law in lawyers' heads[278] will no longer significantly sway developments in a substantive area of law. Instead, crypto-legal developments would be driven more directly by technologists.

2. Cryptolaw Anticipates that Developers Writing Code May Determine Crypto-Legal Culture More than Lawyers

Advanced technology systems, such as predictive technology and DLT, "are sometimes thought to exist independently of human rule-making, and governed only by mathematical algorithms. This is a misconception. Just like legal code, technical code needs to be produced and maintained by humans who define the rules that the code embodies."[279] Lessig put it this way: "If code is law, then . . . 'control of code is power.'"[280] If law is implemented through crypto-legal structures and those crypto-legal structures are written by software developers that control the code, then the culture of those software developers is likely to impact the law. It will be the social reality of the coders and the language of code that influences legal compliance and disputes rather than the social reality of a community of lawyers and their clients. Technologists, untrained in legal theory, being overseen by regulators, many of whom are not lawyers and most of whom cannot read or write computer code, will become the locus of legal culture. What impact will that shift in legal culture have on law practice and legal education? What impact will the shift have on approaches to dispute resolution, motion practice, and discovery strategy? What impact on contract negotiation? Would the shift reduce the frequency with which companies choose business strategies that involve regulatory entre-

278. *See* LoPucki, *supra* note 271.

279. Vili Lehdonvirta & Robleh Ali, *Governance and Regulation*, *in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 40, 43 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [https://perma.unl.edu/5R55-4M3S].

280. LAWS OF CYBERPSACE I, *supra* note 155, at 60 (quoting William Mitchell).

preneurship?[281] The implications of cryptolaw for changing substantive law, reshaping legal structures, and shifting the center of legal culture away from lawyers and toward technologists raises significant challenges, implications, and consequences of adopting crypto-legal structures.

V. CHALLENGES, IMPLICATIONS, AND CONSEQUENCES OF ADOPTING CRYPTO-LEGAL STRUCTURES

This Article predicts that, in areas of law that will benefit from one or more of the elements of the DLT service bundle, transplanting existing legal rules into DLT-based, smart-contracting, semi-autonomous, self-executing, adaptable computer code will simplify substantive law, lead to the emergence of new regulatory actors, shift the locus of legal culture from lawyers to coders, and decrease the lag between law and technology. Even anticipating these changes, however, the emergence of crypto-legal structures will present other challenges, implications, and consequences. This Part identifies three nonexhaustive areas that each merit careful consideration during the construction and implementation of crypto-legal structures and considers the implications and consequences of each for the law. First, a crypto-legal structure will not be appropriate for use in every area of the law; lawmakers and regulators will need to draw boundaries around the cryptolaw's scope. Second, the legal system must prepare to respond to and adjudicate unexpected consequences of crypto-legal structures. Third, because cryptolaw will alter fundamental elements of the legal system, civil society may respond unfavorably to such significant changes and react either by creating a shadow society of noncompliant institutions or by creating alternative public–private distributed-governance partnerships that encourage diverse, endogenous, responsive regulation. Either scenario would have significant implications and consequences for the law.

A. Drawing Boundaries Around Cryptolaw's Scope

This Article does not assert or assume that every aspect of the law is appropriate for transplantation into a crypto-legal structure. The body of cryptolaw that emerges will not likely be one in which the entirety of any given legal system resides in DLT-based computer code. Rather, as explained in section II.A., crypto-legal structures should be

281. For a detailed analysis of the phenomenon of regulatory entrepreneurship, see Pollman & Barry, *supra* note 101. On the theory, which should be explored further, that companies would be less likely to resort to regulatory entrepreneurship if their business culture and language were more readily understood by regulators, regulation implemented by technologists might bridge the communication gap and reduce the need for business models based on regulatory entrepreneurship.

considered for implementation in those areas of law beset by some problem that can be addressed by one or more elements of the core DLT service bundle. Even with that initial limitation, one of the key challenges for cryptolaw will be the challenge faced by regulators in selecting an appropriately ripe legal system for transplantation into crypto-legal structures. Additional criteria that may assist in drawing scope boundaries for emerging crypto-legal structures include: (1) that the legal structure being transplanted into cryptolaw be a concrete legal structure that is part of a concrete legal system; (2) that the legal structure transplanted to cryptolaw not, at least initially, serve a function of physically restraining a person; and (3) that the transplanted legal structure be one of broad-based application rather than one of individual behavior modification.

As to the first criterion, systems analysis is best applied to concrete systems, a system "that exists in 'physical space-time' and is composed of real people and/or other physical objects."[282] The examples of the BSA Regulations and the Article 9 filing systems meet this criterion. The BSA Regulations govern financial institutions and their customers, which are real people and operate in real time and space using real funds. The Article 9 filing system, for its part, governs the interactions between real people regarding property interests in, possession of, and the right to repayment from real objects of personal property, and the filing system itself is managed by an office manned by filing officers reviewing paper files and working on computer hardware. The common law, even if it could otherwise benefit from one or more of the elements of the DLT service bundle, on the other hand, would be an example of a legal system that does not fit this criterion. Instead, as an abstract body of legal rules, the common law is more in the nature of a "conceptual system."[283] The first criterion thus enables lawmakers to consider some legal structures or legal subsystems as out of cryptolaw's scope even when it might otherwise seem to benefit from some aspect of DLT.

As to the second criterion, because crypto-legal structures will self-execute and, as discussed further below, some code choices may lead to unexpected results, legal subsystems that govern physical restraint of people or things should be out of cryptolaw's scope. For example, even if, as part of reforming the Article 9 filing system, DLT could be used to automatically disable some piece of equipment (e.g., farming equipment such as a tractor or construction equipment such as a hoist) so that it would no longer work upon a debtor's default, that function should be beyond the scope of cryptolaw for at least two reasons. First, the code will self-execute upon the debtor's default. The debtor may be in the midst of operating the equipment and it may be dangerous to

282. LoPucki, *supra* note 176, at 488 (footnote omitted).
283. *Id.*

the safety of the debtor or others for the equipment to become disabled during active use. The code will not know the circumstances of the equipment at the time it is disabled, and the code will not care. Second, as further detailed below, coding smart contracts can be difficult and complex, and the more elaborate the coding, the more likely the smart contract may result in unexpected effects. For example, the code may suffer an error that disables the equipment inappropriately and causes new legal problems resulting from what would effectively be an unlawful repossession of the property (a conversion lawsuit, for example), in addition to any threats to the safety of people near to or operating the machinery at the time it became disabled. As to the third criterion, Anthony Casey and Anthony Niblett suggest that increasing use of technology in the design, implementation, and enforcement of law may encroach on the privacy, autonomy, and ethical domain currently reserved for individuals.[284] This may suggest that crypto-legal structures are better suited for broad-based legal systems and subsystems, such as the BSA Regulations and the Article 9 filing system, and less appropriate for enforcing compliance with crosswalk signals, traffic lights, and other rules governing individual behavior.

Applying these criteria when selecting legal structures ripe for transplantation into crypto-legal structures will not wholly eliminate the challenge of defining cryptolaw's scope. Other criteria for consideration will emerge organically as initial crypto-legal structures are developed. Further, as initial crypto-legal structures are implemented, in keeping with the prediction of legal-transplant theory, the crypto-legal structures may not behave as intended or expected. The unexpected results will not automatically signal that the crypto-legal structure failed but may give rise to both new challenges related to the scope of cryptolaw and related to other aspects of creating and implementing crypto-legal structures.

B. Expecting Unexpected Results

Correctly coding smart contracts to accomplish the task desired in the manner desired can be especially difficult as compared to traditional software programming.[285] Furthermore, the nature of DLT is such that even a small error can have significant effects.[286] The ex-

284. Casey & Niblett, *supra* note 16, at 49–54.

285. KEVIN DELMOLINO ET AL., STEP BY STEP TOWARDS CREATING A SAFE SMART CONTRACT: LESSONS AND INSIGHTS FROM A CRYPTOCURRENCY LAB, http://fc16.ifca.ai/bitcoin/papers/DAKMS16.pdf [https://perma.unl.edu/6Y4K-T3H2] ("Our lab experiences show that even for very simple smart contracts (e.g., a 'Rock, Paper, Scissors' game), designing and implementing them correctly was highly non-trivial.").

286. *Id.* ("In contrast to traditional software development tasks where bugs such as buffer overflows are often benign (except in rare or contrived scenarios), in our lab, we observed several bugs and pitfalls that arise due to the unique nature of

ploit of a flaw in the code of The DAO[287] offers a clear example of complex smart contracting computer code leading to unexpected results.[288] The DAO essentially operated as a decentralized venture-capital fund,[289] "borne from immutable, unstoppable, and irrefutable computer code, operated entirely by its members, and fueled using ETH."[290] One of its participants exploited a known bug (that programmers were actively working to fix) in The DAO's code to divert 3.6 million ether (ETH), roughly valued at fifty million dollars, into a "child DAO" that only that participant controlled.[291] The ongoing dispute regarding how to respond to the exploit is beyond the scope of this Article.[292] The relevance here is that even some of the most sophisticated coders in the field[293] were surprised by unexpected effects of the computer code they had created. This has important implications for the possibility of using DLT to code self-enforcing, semi-autonomous legal rules.

---

smart contract programs and lead to clear and immediate exploits (e.g., theft or loss of money).").

287. David Siegel, *Understanding the DAO Attack*, COINDESK (June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists [https://perma.unl.edu/937A-6BH4] ("A DAO is a Decentralized Autonomous Organization. Its goal is to codify the rules and decisionmaking apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control. . . . 'The DAO' is the name of a particular DAO, conceived of and programmed by the team behind the German startup Slock.it—a company building 'smart locks' that let people share their things (cars, boats, apartments) in a decentralized version of Airbnb.").

288. Paul Vigna, *Chiefless Company Rakes in More than $100 Million*, WALL STREET J. (May 16, 2016), http://www.wsj.com/articles/chiefless-company-rakes-in-more-than-100-million-1463399393.

289. David Z. Morris, *Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, and Counting*, FORTUNE (May 15, 2016), http://fortune.com/2016/05/15/leaderless-blockchain-vc-fund [https://perma.unl.edu/YF7Q-TLD8].

290. Matt Levine, *Blockchain Company Wants to Reinvent Companies*, BLOOMBERG VIEW (May 17, 2016) (quoting The DAO's "Principles" page, which is no longer available), https://www.bloomberg.com/view/articles/2016-05-17/blockchain-company-wants-to-reinvent-companies [https://perma.unl.edu/JT79-V8M8].

291. Siegel, *supra* note 287.

292. For more information on the aftermath of the "hack" and the proposed responses, see generally Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (July 20, 2016), http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds [https://perma.unl.edu/D5RX-MXT8]; Siegel, *supra* note 287.

293. DIEDRICH, *supra* note 8, at 54 ("Christoph Jentzsch, who programmed The DAO—which was subsequently hacked and lost $50,000,000—is an Ethereum veteran with a university degree in theoretical and mathematical physics. He is not a seasoned coder or software system architect. But he is a smart guy who understands Ethereum. He even had professional experience as a software tester. But decentralized code can be exceedingly hard to test. That even he can trip up, predicts that a lot of people trying their hands at smart contracts will.").

If The DAO's code was a crypto-legal structure, the exploit and the resulting diversion of funds to the child DAO would have called into question the role of the regulators that oversaw the transplant of the existing legal structure into DLT and any resulting civil or other liability for their actions in that role. To be held responsible, the regulators filling the role must be able to work with the coders, understand the work as it is ongoing, and be proficient enough in coding to be able to conduct an independent review of the crypto-legal structure after it has been created. Similarly, for a citizen affected by a bug or exploit of a crypto-legal structure, to pursue any rights he or she may have in relation to the problem, the citizen's attorney must be proficient enough in computer coding and DLT to effectively assess the evidence and craft a legal strategy. Thus, to expect the unexpected results for which legal-transplant literature instructs us to prepare, we need regulators and attorneys that can write, read, and understand computer code. This implication of cryptolaw will have important effects on the legal profession that extend beyond the changes to the fundamental elements of the legal system discussed in Part II above, suggesting that it merits its own treatment in separate work.

C. Cryptolaw Will Encourage Discourse Regarding Alternative Governance Models

> The existence of the regulatory state, as well as the availability of civil and, potentially, criminal avenues for the redress of grievances, are so much with us that we accept them as given: we presume that government and its various agents exist to serve as buffers—to protect us from harms beyond our control—and that there will always be a way in which to seek a remedy against or to prosecute those who have done us harm.[294]

This customary approach of the governed to interact with the laws by which they are governed is shaped by the legal structures themselves. The two are connected. As cryptolaw causes subtle shifts in substantive law, legal structures, and legal culture, the governed may chafe against the weight of automatically executing laws that shape their daily activity. Furthermore, as cryptolaw works to overcome its challenges and society confronts the implications of its existence, society may discover that carrying law and regulation to its logical conclusion through semi-autonomous, self-executing computer code reveals deep-seeded flaws in the law or the theory underpinning the law in clearer ways than ever before. In either case, civil society may respond in one of two ways: (1) build a separate set of institutions that do not incorporate crypto-legal structures and effectively operate in a shadow society or (2) push for more endogenous forms of governance models at a vari-

294. Lawrence Friedman, *Digital Communications Technology and New Possibilities for Private Ordering*, 9 ROGER WILLIAMS U. L. REV. 57, 60–61 (2003) [hereinafter Friedman, *Digital Communications Technology*].

ety of levels, including political, social, business, and corporate governance. Although the second option is normatively preferable, the first has historical precedent and is likely easier to create an alternative to forced compliance with law through crypto-legal structures. It is also entirely possible that both possibilities emerge simultaneously, radically altering the enforcement landscape.

If civil society responds to the challenges and unexpected consequences of cryptolaw with disfavor, a significant portion of civil society may opt not to use crypto-legal structures. Civil society actors may instead opt to build noncompliant businesses, communities, and commerce models. In other words, in a world where the law prefers crypto-legal structures that some part of the governed disfavor, a shadow society of noncompliant people, entities, commerce, and communities may emerge. The emergence of this shadow society will require lawmakers and regulators to determine: (1) whether any penalty for failure to use the crypto-legal structure will be imposed; (2) if so, what kind of penalty; and (3) how to determine when the penalty applies in the face of constitutional defenses such as exercise of speech or religion, or constitutional criminal protections.[295] Lawmakers and regulators will also be called upon to determine whether the shadow society's existence has any societal, socioeconomic, or social justice implications that render cryptolaw a less desirable form of law than first estimated. None of these issues are new to the law, but they will be new in a law-and-technology context that will have already shifted some of the fundamental elements of the system by implementing crypto-legal structures.

The second possibility is that new, more creative forms of partnered governance will emerge using DLT. Although a call for more transparent, more citizen-responsive law is not new, DLT will offer average citizens greater opportunity to create, manage, and widely disseminate governance models that better reflect their interests, values, and goals.[296] After experiencing the power of DLT when it is backed by the power of the state, some groups may be emboldened to attempt more elaborate forms of governance through private ordering using a private form of crypto-legal structures. Such a phenomenon has loosely developed in the context of the Internet.

As Friedman explained, "[I]n addition to enabling new forms of interpersonal communication, [the Internet] has also become a social

295. *See, e.g.*, Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013) (arguing that First Amendment law may need to be adjusted to address decisions based on algorithms); Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871 (2016) (analyzing Automated Suspicion Algorithms under the Fourth Amendment).

296. For an example of a platform experimenting with this, see BACKFEED, http://backfeed.cc [https://perma.unl.edu/ZM3J-8LJY].

space whose discrete sectors feature their own developing norms of regulation and redress, many of which depart from their physical world analogs."[297] The private ordering taking place on the Internet, of course, simply represents a technologically enhanced version of the same phenomenon that repeatedly appears in different communities throughout history. For example, *lex mercatoria* represented a global set of norms created by merchants for use in conducting affairs with other merchants across the globe during the Middle Ages.[298] A private law of international commerce,[299] a law merchant for the Internet (*lex informatica*),[300] and other examples abound.[301] Aaron Wright and Primavera de Filippi already predict the emergence of private rules systems in DLT.[302] Arguably, the *lex cryptographia* that they predict, however, will be limited to specialized groups proficient in DLT or operating DLT-related businesses. The question then becomes whether and how the experience of such specialized groups in building private systems to govern their affairs will meld with the more public, state-backed form of lawmaking through DLT. In other words, how might public law, or state-backed law, begin to form through private ordering? Could DLT enable communities to endogenously build and propose norms and rules that, through crypto-legal structures, possess more than mere "soft power" in their communities? In doing so, could cryptolaw allow more diversity in substantive and procedural law that

297. Friedman, *Digital Communications Technology, supra* note 294, at 61 (citing David H. Gleason & Lawrence Friedman*, Toward an Accessible Conception of Cyberspace*, 28 VT. L. REV. 299 (2003)).

298. Ralf Michaels, *The True Lex Mercatoria: Law Beyond the State*, 14 IND. J. GLOBAL LEGAL STUD. 447, 448 (2007) ("The first stage concerns an ancient lex mercatoria in the Middle Ages, a transitional set of norms and procedural principles, established by and for commerce in (relative) autonomy from states." (citing HAROLD J. BERMAN, LAW AND REVOLUTION: THE FORMATION OF THE WESTERN LEGAL TRADITION 332–56 (1983); LEX MERCATORIA AND LEGAL PLURALISM: A LATE THIRTEENTH-CENTURY TREATISE AND ITS AFTERLIFE (Mary Elizabeth Basile et al. eds., 1998))).

299. *Id.* at 448 ("The second stage describes the renaissance of the idea as a 'new lex mercatoria' in the 20th century, an informal and flexible net of rules and arbitrators establishing a private international commercial law." (citing J.H. Dalhuisen, *Legal Orders and Their Manifestation: The Operation of the International Commercial and Financial Legal Order and Its Lex Mercatoria*, 24 BERKELEY J. INT'L L. 129 (2006))).

300. *See generally* Aron Mefford, *Lex Informatica: Foundations of Law on the Internet*, 5 IND. J. GLOBAL LEGAL STUD. 211 (1997) (describing an independent, or private, system of law for governing transactions on the Internet).

301. *See e.g.*, JEROLD S. AUERBACH, JUSTICE WITHOUT LAW? 27–28 (1983) (looking at the experience of seventeenth-century American colonists in using nonlegal dispute resolution); ROBERT C. ELLICKSON, ORDER WITHOUT LAW (1991) (detailing how the community of cattle ranchers in Shasta County, California, used private ordering to govern inter-neighbor affairs).

302. *See generally* Wright & De Filippi, *supra* note 19.

better reflects the communities that it governs and the socioeconomic realities that those communities face?[303]

VI. CONCLUSION

Using comparative law as a methodological paradigm, this Article conceptualizes the contours of a new legal discourse regarding the impact on the legal system resulting from the use of DLT to implement, enforce, and adjudicate law. In so doing, this Article predicts that the current fledging phenomenon of creating crypto-legal structures will expand in the near and long term, and argues that such DLT-enabled law is poised to change the basic structures of any legal system using it, including basic ideas about the nature of law and the process of adjudication. Recognizing that DLT is not a panacea, this Article first confines cryptolaw to a discussion about the application of DLT to problems in lawmaking, regulation, and enforcement that relate to the law's inability to enable actors to reach a consensus about the existence and evolution of shared facts. Further, the Article recognizes that some areas of the law will be better suited to crypto-legal structures than others because of their concrete nature. Within those boundaries, however, those designing crypto-legal structures should feel free to remedy the problem with whichever combination of the five elements of the blockchain service bundle is deemed appropriate under the circumstances.

With these preliminary boundaries of the cryptolaw discourse in mind, the Article uses comparative law as a framework for predicting other important areas of discussion and inquiry. First, creating crypto-legal structures should be thought of as an exercise in legal transplantation, transplanting a law into the foreign legal system of DLT computer code. As legal transplantation, those designing crypto-legal structures should use functional equivalents in the code as an opportunity to simplify substantive law. The legal system using crypto-legal structures should also prepare for the emergence of new, and sometimes unexpected, results, including the emergence of new regulatory actors. Cryptolaw offers a way to think about these new elements, anticipating specifically the impact of self-executing elements of the computer code and the software developers that create the crypto-legal structures. Cryptolaw also offers a framework for considering the impact of crypto-legal structures on legal culture, suggesting that the gap between the law in action and the law in the

303. These questions suggest the emergence of new crypto-governance models. Several areas are ripe for exploration of such models: corporate governance, contract theory, public and community governance models, and law-and-development theory, to name a few. Each such area deserves its own thorough examination. I mention them here only to emphasize the far-reaching implications of cryptolaw's potential effect on governance through legal and other mechanisms.

books may disappear and that legal culture itself may change as the increased involvement of software developers eliminates the role of individual legal professionals interpreting law in the field.

In sum, by offering an initial picture of the impact on legal systems of a world using crypto-legal structures to address perceived inefficiencies and complexity in the law, this Article launches a new discourse. This new cryptolaw discourse will stand on its own as a new field of legal academic inquiry and area of legal practice. It will develop new substantive questions of law, issues for adjudication, and name new types of legal actors. Notably, the cryptolaw discourse will require interdisciplinary discussion. First, cryptolaw will disrupt other adjacent areas of law, such as administrative law, commercial and corporate law, contracts, and torts, among others. Second, overcoming the challenges and accounting for the collateral implications and consequences of using crypto-legal structures will require increased dialogue between those trained in the disciplines of law and policy and those trained in the disciplines of computer science and mathematics. To realize the potential of crypto-legal structures for increasing efficiency, transparency, and equity in governance, this Article calls upon those currently designing crypto-legal structures for governments and public–private partnerships to first undertake a cryptolaw analysis of the type conceptualized here. Ultimately, the idea that new, more transparent, more endogenous, more culturally appropriate governance models might emerge in response to challenges arising from using crypto-legal structures hints at the true expanse of cryptolaw's promise: although every law and legal theory continually evolves in an effort to better serve the governed, cryptolaw offers a legal discourse that anticipates doing so more rapidly, more efficiently, more transparently, and in new and creative ways that may encourage increased civic engagement.