BITPROPERTY

JOSHUA A.T. FAIRFIELD[*]

ABSTRACT

Property is the law of lists and ledgers. County land records, stock certificate entries, mortgage registries, Uniform Commercial Code filings on personal property, copyright and patent registries of interests in intellectual property, bank accounts, domain name systems, and consumers' Kindle e-book collections in the cloud are all merely entries in a list, determining who owns what.

Each such list has suffered a traditional limitation. To prevent falsification or duplication, a single entity must maintain the list, and users must trust (and pay) that entity. As a result, transactions must proceed at significant expense and delay. Yet zero or near-zero transaction costs are the fuel of Internet scalability. Property transactions have not yet truly undergone an Internet revolution at least partly because they are constrained by the cost of creating centralized trusted authorities.

This Article reimagines the contours of digital property if that central constraint were removed. There is every reason to believe it can be. Increased interest in cryptocurrencies has driven the development of a series of technologies for creating public, cryptographically secure ledgers of property interests that do not rely on trust in a specific entity to curate the list. Previously, the digital objects that users could buy and sell online were not rivalrous in the same way as offline physical objects, unless some centralized entity such as a social network, digital currency issuer, or game

* Professor of Law, Washington and Lee University School of Law. Thanks to the participants at the Digital Asset Transfer Authority 2014 meeting, the 2014 ACI Virtual Currency conferences, the Conference of State Bank Supervisors, and the SEALS Panel on Neo-Technological Property Theories for input and improvement. Thank you in particular to Juliet Moringiello and James Grimmelmann for comments and suggestions. Thank you to Google's Mike Shick for the dice-rolling metaphor for SHA-256. Thanks to Hannah Shtein, Natalie Wengroff, and Paul Keith for research assistance, and to the Frances Lewis Law Center for support during the drafting of this piece.

company served the function of trusted list curator. Trustless public ledgers change this dynamic. Counterparties can hand one another digital, rivalrous objects in the same way that they used to hand each other gold bars or dollar bills. No intermediary or curator is needed.

In addition, the advent of this technology provides an opportunity to discuss property interests in information environments. Property online is currently anemic. Consumers control few online resources and own even fewer. This is in no small part due to antiquated notions of property as the law of physical, tangible resources. Given new technology that can create digital, scarce, and rival intangible assets, these basic assumptions should be reexamined and replaced with a theory of property as an information communication and storage system. That is the project of this piece.

TABLE OF CONTENTS

INTRODUCTION 807
I. TRUSTLESS TECHNOLOGY 812
  A. TRUSTLESS PUBLIC LEDGERS 813
  B. BITS AND BOLTS 816
    1. How Trustless Public Ledgers Work 817
      a. The Double-Spending Problem 817
      b. The Public Ledger Solution 819
      c. Network Effects and Vulnerabilities 823
    2. Tokenized Property 825
    3. Protocol Networks and Side-Chains 828
  C. USE CASES AND REGULATORY REGIMES 829
    1. Currency and Payments 831
    2. Property 834
II. BITPROPERTY 838
  A. PROPERTY AS A LAW OF INFORMATION 842
    1. Property and Information Cost Theory 844
    2. Property, Information, and Modularity 847
    3. Property Is a Law of Information, Not Things 849
      a. Thing-ness in Property Law 850
      b. Object Oriented Programming 852
      c. Object Oriented Property 853
  B. THE PROPERTY PROTOCOL 854
    1. Data Formatting 857
    2. Verification and Error Checking 859

3. Data Security 860
III. OPERATIONALIZING BITPROPERTY 863
A. NECESSARY ADJUSTMENTS TO CURRENT THEORY 863
1. Disentangling Tangibility 864
2. Differentiating Digital and Intellectual Property 865
3. Establishing Block Chain Neutrality 869
B. CONCEPTUAL CHALLENGES 870
1. Is Information Separate from Property? 870
2. Is Information Subordinate to Property? 871
3. Is All Information Property? 872
CONCLUSION 873

INTRODUCTION

Property is the law of lists and ledgers. The vast bulk of owned wealth is recorded in systems that tell users who owns what.[1] County courthouse land records, Uniform Commercial Code ("UCC") security interest filing systems, electronic chattel paper, the stock clearing house system, the Mortgage Electronic Registration System ("MERS"), Automated Clearing House ("ACH") transactions, bank accounts, intellectual property interests filed with federal registries, and consumer-purchased music through iTunes are all just entries in a ledger associating an identity with an interest in a resource.[2]

This Article explores the practical and theoretical ramifications of recent advances in ledgers used to track and convey property interests.

1. Christopher L. Peterson, *Foreclosure, Subprime Mortgage Lending, and the Mortgage Electronic Registration System*, 78 U. CIN. L. REV. 1359, 1363–64 (2010) ("Public land title records have been a fundamental feature of American law since before the founding of the Republic. . . . Perhaps then, it is not surprising that in the early seventeenth century, Americans began experimenting with laws requiring that parties create public records of conveyances and mortgages.").

2. *See, e.g.*, JANE K. WINN & BENJAMIN WRIGHT, LAW OF ELECTRONIC COMMERCE § 9.03 (4th ed. 2013) ("In 2004, MERS extended the scope of its services by creating an 'eRegistry' to establish a central registry of interests in 'eNotes' or electronic promissory notes used in residential real estate transactions."); Juliet M. Moringiello, *False Categories in Commercial Law: The (Ir)relevance of (In)tangibility*, 35 FLA. ST. U. L. REV. 119, 124–25 (2007) [hereinafter Moringiello, *False Categories*] ("Articles 7 and 9 of the U.C.C. now provide for electronic documents of title and electronic chattel paper, respectively . . . ."); David W. Opderbeck, *The Penguin's Genome, or Coase and Open Source Biotechnology*, 18 HARV. J.L. & TECH. 167, 224 (2004) ("[Some of] the information that prospective licensees and licensors need to enter into efficient transactions . . . already exists in public intellectual property registries, such as those maintained by the U.S. Patent and Copyright Offices.").

Bitcoin is a rapidly developing digital currency.[3] The underlying technology (called the "block chain")[4] has nothing in particular to do with money, however. Block chain technology instead represents a significant advance in tracking information about who owns what. It does so through a distributed public ledger that does not require trust in other parties or in a central list authority, and is robustly resistant to falsification.[5] As venture capitalist Marc Andreessen wrote for the *New York Times*:

> Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.[6]

Most of the discussion in the legal literature and news media to date has centered around the use of such public ledgers as a substitute for currency.[7] However, a distributed public ledger system confers not just the power to transfer dollars, but also the power to transfer anything:

> What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks,

---

3. This Article is more concerned with the underlying technology of public ledgers than it is with the success or failure of the specific implementation of Bitcoin. Thus, questions of the volatile price of Bitcoin or other concerns related to the success of that specific implementation are given limited attention in this piece.

4. *See infra* notes 30, 36–37 and accompanying text.

5. Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 116 (2012).

6. Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters.

7. *See generally* Paul H. Farmer, *Speculative Tech: The Bitcoin Legal Quagmire and the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85 (2014) (outlining the legal implications of categorizing Bitcoin as a currency); Jordon L. Ludwig, Note, *Protections for Virtual Property: A Modern Restitutionary Approach*, 32 LOY. L.A. ENT. L. REV. 1 (2012) (discussing disputes over property in virtual worlds); Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159 (2012) (discussing whether Bitcoin can be a sustainable currency); Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813 (2014) (discussing the regulation of cryptocurrencies); Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. 1483 (2014) (discussing Bitcoin as a substitute for traditional financial systems); Kaplanov, *supra* note 5 (discussing the regulation of Bitcoin); Ruoke Yang, *When is Bitcoin a Security Under U.S. Securities Law?*, 18 J.L. TECH. & POL'Y 99, 108 (2013) (discussing whether Bitcoin is a security); Derek Dion, Note, *I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash*, U. ILL. J.L. TECH. & POL'Y 165 (2013) (discussing the regulatory policy implications for Bitcoin); Joshua Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119 (2013) (discussing the merits of Bitcoin as a digital currency); Danton Bryans, Note, *Bitcoin and Money Laundering: Mining for an Effective Solution,* 89 IND. L.J. 441 (2014) (discussing the money laundering implications for Bitcoin).

> or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds . . . and digital money.[8]

Thus, "[f]or the first time, two people can exchange a piece of digital property, without any prior relationship, and in a secure way, over the Internet."[9] This functionality extends well beyond the use of trustless ledgers as online money. "The breakthrough means that, theoretically, any act of commerce on the Web can be decentralized and stripped of a controlling authority."[10] The ability to disintermediate and decentralize significant portions of online activity can significantly disrupt and improve online ownership and the legal regimes that govern it.[11]

This Article addresses the potential for change in property law and the accompanying needed changes to property theory. Trustless ledgers offer the potential to significantly address one of the great inefficiencies of modern property: its reliance on expensive, inaccurate, hard-to-access, hard-to-search, and insecure ledgers of all stripes.[12] Trustless technology can significantly reduce information costs and increase certainty across the law of property.[13] Dusty and unsearchable courthouse land records can be made public and verifiable, and bank accounts can be made fully traceable, even down to the pennies, over years' worth of time.

At the outset, one caveat is important. The success or failure of Bitcoin in particular is ultimately of only passing interest.[14] "Bitcoin is an experiment," noted developer Gavin Andresen, and "maybe it will change the world, but realise that investing . . . in new ideas is always risky."[15] It is

8. Andreessen, *supra* note 6.

9. Rob Wile, *Satoshi's Revolution: How the Creator of Bitcoin May Have Stumbled Onto Something Much, Much Bigger*, BUS. INSIDER (Apr. 22, 2014, 11:50 AM), http://www.businessinsider.com/the-future-of-the-blockchain-2014-4 (quoting interview with Bitcoin developer Jeff Garzik).

10. *Id.*

11. *See* Pete Rizzo, *VC Fred Wilson: Block Chain Could Be Bigger Opportunity than Bitcoin*, COINDESK (May 5, 2014, 4:58 PM), http://www.coindesk.com/vc-fred-wilson-block-chain-bigger-opportunity-bitcoin (Fred Wilson, founder of Union Square Ventures, discussing the block chain's potential for disruptive innovation outside of the currency and payment spaces).

12. *See* Kaplanov, *supra* note 5, at 116 ("The bitcoin technology ensures that online transactions are: (1) secure; (2) efficient; and (3) free of third party presence—whether that third party is a government, bank, payment network, or clearinghouse.").

13. *See id.* at 125 ("By creating a two-party payment system for online transactions, the cost of the transaction is reduced, thereby nearly eliminating the added costs to the consumer.").

14. *Virtual Currencies: Mining Digital Gold*, ECONOMIST (Apr. 13, 2013), http://www.economist.com/news/finance-and-economics/21576149-even-if-it-crashes-bitcoin-may-make-dent-financial-world-mining-digital.

15. *See Virtual Currency Schemes*, EUR. CENT. BANK 27 (Oct. 19, 2012), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (quoting Gavin Andresen, *That Which Does Not Kill Us Makes Us Stronger*, GAVINTHINK (June 20, 2011, 11:56 AM),

probable that security flaws in trustless public ledgers, their infrastructure, or their implementation will be discovered. Some already have been. This Article analyzes the potential for the technology to impact online property regimes, not the soundness of any one implementation. Thus, as *The Economist* noted, "[j]ust like Napster, Bitcoin may crash but leave a lasting legacy."[16]

Instead of offering a paean to Bitcoin, this Article makes use of the advent of this potentially disruptive technology[17] to reflect on property theory,[18] which has badly and barely managed the transition to the online ecosystem.[19] Whereas contract and tort law have survived the digital transition more or less intact, online property interests are either intellectual property interests or strange amalgams of contract, licensing, and pseudoproperty law, such as those that govern users' interests in e-books, MP3s, software, or downloaded movies.[20] Traditional property law, with its virtues of simplicity, modularity, decentralization, disintermediation,

http://gavinthink.blogspot.com/2011/06/that-which-does-not-kill-us-makes-us.html).

16. *Virtual Currencies: Mining Digital Gold*, *supra* note 14. *See also* Michael Sivy, *The Real Significance of the Bitcoin Boom (and Bust)*, TIME (Apr. 12, 2013), http://business.time.com/2013/04/12/the-real-significance-of-the-bitcoin-boom-and-bust/ ("But the Bitcoin phenomenon is more than a bubble. It says something important about the current and future state of the global economy. . . . However the current boom-and-bust plays out, Bitcoin is the beginning of something, not the end."); T.S., *The Economist Explains: How Does Bitcoin Work?*, ECONOMIST (Apr. 11, 2013, 11:50 PM), http://www.economist.com/blogs/economist-explains/2013/04/economist-explains-how-does-bitcoin-work ("Just as BitTorrent was not the first file-sharing service and Skype was not the first voice-over-internet service, it may be that Bitcoin will be a pioneer in the field of virtual currencies, but will be overshadowed by an easier-to-use rival.").

17. Disruption in the technological context means a technological advance that unsettles legacy actors in an area, permitting new entrants to gain traction in the market. CLAYTON CHRISTENSEN, THE INNOVATOR'S DILEMMA: WHEN NEW TECHNOLOGIES CAUSE GREAT FIRMS TO FAIL xv–xvi (1997).

18. *See, e.g.*, Rhys Bollen, *The Legal Status of Online Currencies: Are Bitcoins the Future?*, 24 J. BANKING & FIN. L. & PRAC. 272, 279 (2013) ("Bitcoins are a form of intangible private property, a valuable digital artefact. They are not a contractual promise by or debt owed by one party to another. They are an asset and are the valuable property of their current owner, who can transfer them as and when she pleases.").

19. *See, e.g.*, Moringiello, *False Categories*, *supra* note 2, at 120 ("Classifying property according to its tangibility or intangibility creates false categories unrelated to significant legal distinctions, and these false categories hinder the ability of commercial law to expand to adequately accommodate electronic assets.").

20. *See id.* (arguing that moving away from the distinction between tangible and intangible assets in property law "will allow commercial law to more readily adapt to the proliferation of emerging electronic assets that do not fit into established categories of intangible rights such as intellectual property and payment rights"); Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047, 1052 (2005) [hereinafter Fairfield, *Virtual Property*] ("[U]nreasonable contractual restraints on alienation are eliminated by the law of property. But currently in the context of the internet, we have imported the common law of contract wholesale, without the counterbalance of property law. As a result, emergent useful property forms are being eliminated by contract.").

equalization, independence, and certainty, has not made the transition well.[21] Until recently, it has been hard, even impossible, to own a digital object in the same way that one owns a car or a farm. That impossibility has now begun to give way to human ingenuity, and so theorists must make straight the way for true digital ownership interests.

Property law is ripe for an information revolution. Information applications scale rapidly when costs fall.[22] Property has not benefitted from the scaling effect of drastically reduced information costs because property law has been traditionally understood as being concerned with tangible objects, rather than information. The perhaps oversimplified statement of the problem is that one cannot send property over the Internet. Given the robust trade in digital objects, this is demonstrably not true, but there is a deeper issue. The very first move of property is to dissociate the property interest from the object. Property does not consist in the thing itself; rather, property consists in the packaging, tracking and transmission of information about the dissociation between interest and resource. The property interest, being information, can of course be conveyed using information systems. In short, property law is not primarily concerned with things, but with information. Structuring, streamlining, packaging, transmitting, storing, searching, and verifying this information is the work of property law.

From this perspective, then, property is information: who owns what.[23] Of course, property captures more interests than bare ownership, but the rule generalizes: property can be usefully viewed as that set of information describing who may do what, when, and with which resource. Good property rules are ones that package, convey, transmit, or verify such information in ways that reduce information costs, and a good property system is one that communicates this information and transfers the attached resources to new identities with minimal friction.[24] One can rate good property systems by how well they store and communicate information about who owns what, and can identify poor property systems by how much noise and confusion their information search, storage, and transfer

21. *See generally* Moringiello, *False Categories*, *supra* note 2 (arguing that classifying property according to its tangibility poses challenges for classifying electronic assets).

22. Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343, 347–48 (2008) ("The Internet fosters innovation by eliminating transaction costs, enabling new services to emerge.").

23. *See* Moringiello, *False Categories*, *supra* note 2, at 125–41 (discussing what may or may not be property under UCC Section 9).

24. *See, e.g.*, Werbach, *supra* note 22, at 348–49 (discussing how the Internet has benefitted from economies of scale, allowing users to capitalize on existing resources with minimal friction).

protocols create.[25]

A theory of property as information has serious advantages over prior conceptions. It permits the extension of traditional property rules to digital and smart property, and avoids the false constraints of current theory.[26] For instance, it simply does not matter whether the property one considers is tangible or intangible.[27] Whether I hold a physical dollar in my hand or hold a dollar credited in a bank account makes no practical difference.[28] That false distinction has long bedeviled property theory and has particularly impeded the growth of robust markets in online property.[29] A theory of property as information puts paid to these notions. It makes clear that property is an information application, best understood through the lens of information theory. As a result, traditional property law is entirely practicable in information environments.

This Article proceeds as follows. Part I describes trustless public ledger technology, with a particular focus on block chain technology and the nascent regulatory regimes surrounding it. Part II makes the case for treating property as a protocol for communicating and storing information, and demonstrates how property can function well in information environments. Part III offers some concrete suggestions as to how block chain technology could, combined with advances in theory, lay the foundation for a powerful and flexible system for digital property.

I. TRUSTLESS TECHNOLOGY

This part discusses technology that strongly reduces information costs in online property systems. The following sections provide a brief overview of how trustless technology creates the possibility for rapid Internet scaling of property applications, before describing the technical details of implementing a trustless system through the expedient of a public ledger.

25. *See* Abraham Bell & Gideon Parchomovsky, *A Theory of Property*, 90 CORNELL L. REV. 531, 552 (2005) ("[A] property system with stable rights increases the value of assets to users (now owners) and decreases the costs of obtaining and defending those assets.").

26. *See generally* Moringiello, *False Categories*, *supra* note 2.

27. *See id.* at 137, 141 ("Despite the fact that individuals commonly think of intangible rights embodied in almost worthless tangible things as property, intangible rights unconnected to tangible things continue to confound judges. . . . The intangible nature of assets . . . seems to blind courts to general property principles.").

28. Juliet Moringiello, *What Virtual Worlds Can Do for Property Law*, 62 FLA. L. REV. 159, 176 (2010) [hereinafter Moringiello, *Virtual Worlds*] ("In a sense, all money is virtual."); Moringiello, *False Categories*, *supra* note 2, at 136 ("Most of us would consider our bank accounts to be our property notwithstanding the intangibility of the bank account.").

29. *See id.* at 141–43 (discussing how the intangibility of online assets has caused confusion in the courts).

The discussion continues with a description of the different possible use cases for trustless architectures and the regulatory regimes that have to date been brought to bear. Bitcoin as a specific implementation, and the technological characteristics of that specific implementation, are only discussed here insofar as they help the reader understand the core points about digital property and trustless public ledgers.[30]

A. TRUSTLESS PUBLIC LEDGERS

The primary information cost in online property systems is trust. Users must trust that any registry or ledger of property rights is accurate and secure. These verification costs are generally paid by users to a centralized authority that maintains the register of rights. Trustless ledgers, by contrast, are a communications protocol that reduces information costs by eliminating the need for trust in a central curator. Such ledgers enable peer-to-peer digital property transactions without intermediaries.[31] This is the concept of trustlessness.

As an example, one might consider the balance in a bank account. The account itself is a mere entry in a private ledger maintained by the bank. Trust in the bank account depends on trust in the bank.[32] If trust in the bank fails, the bank account is no longer a store of value, but a useless entry on the bank's ledger. Parties can trust such centralized ledgers only as far as they can trust the centralized authority.[33] In the case of bank deposit accounts, such trust might be justified. In the case of 1980s-era Savings and

30. A few definitions apply throughout. The term "trustless" is used here to encompass a band of extremely low-trust applications based on a distributed public ledger that is secured by an effective proof system to ensure the integrity of the ledger despite its decentralization. Note that "trustless" does not imply a lack of trust in the system. To the contrary: it implies that the system is sufficiently trustworthy that no one actor within the system needs to be trusted for the system to work. "Block chain" refers to a kind of public ledger that relies on a distributed proof system to prevent falsification or double spending. The term "block chain" can refer either to the Bitcoin block chain, or to the block chain underlying an alternative chain application. When referred to in the singular, "the block chain" refers to the Bitcoin block chain. "Bitcoin" itself refers to the currency implementation—just one example of trustless public ledger architecture, although it is by far the best-known example. This terminological distinction between Bitcoin and the underlying block chain is important, because it is precisely that distinction that permits innovators to envision building non-currency applications using trustless public ledger architecture.

31. *See, e.g.*, Barrett Sheridan, *Bitcoins: Currency of the Geeks*, BLOOMBERG BUS. (June 16, 2011), http://www.businessweek.com/magazine/content/11_26/b4234041554873.htm (explaining how Bitcoin transactions do not require a "middleman").

32. *See* Moringiello, *Virtual Worlds*, *supra* note 28 at 176 ("Money is based on trust; currency has value because people trust that it can be exchanged for items of value and other currencies.").

33. *Virtual Currency Schemes*, *supra* note 15, at 9–10 ("People are willing to accept [currency] in exchange for goods and services simply because they trust this central authority. Trust is therefore a crucial element of any fiat money system.").

Loans, it would not. Trust in the ledger entry of a bank account is only as good as the trust in the institution that maintains it.[34]

Enormous resources currently go into generating trust, which makes trust-based systems expensive.[35] To maintain trust, the centralized authority must restrict access to the ledger, while itself submitting to expensive (but necessary) oversight to ensure its own trustworthiness. If just anyone could change the ledger, under the traditional system, trust would evaporate. Even if one were inclined to trust the centralized administrator, one could not possibly trust everyone who could make changes to the centralized ledger. Consider, for example, a case in which all customers were free to edit their bank account balances at will. This would reduce the transaction and processing costs of maintaining the ledger system (since the bank would not have to pay for systems and people to do so) but would also destroy trust in the system.

Trustless public ledgers are a proposed solution to the problem of expensive trust. Bitcoin is the best known implementation, and thus serves as a good example here. 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."[36] The block chain is not maintained by any single entity, but instead relies on a mathematically innovative consensus model.[37] Bitcoin creates a manipulation-resistant solution to the problem of trust—a way of providing verification without centralization and its attendant risks and costs. This mechanism is discussed at more length in Section I.B, below.

Trustless public ledger systems are of course neither entirely devoid of trust[38] nor completely zero cost.[39] The systems propose only to significantly reduce the need for trust and its associated costs. Reduction of the need for trust eliminates a constant source of friction in online transactions. Internet technologies scale most disruptively at near-zero

34. *See id.*

35. *See generally* Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. REV. 457, 474–76 (2001).

36. *See supra* note 30 (defining "block chain").

37. *See* Sheridan, *supra* note 31 (discussing the mechanics of Bitcoin).

38. For example, even if one does not trust a central authority, one might trust the implementation of the protocol, the actors who implement the protocol, or the essential mathematical soundness of the protocol itself in the face of sustained and highly motivated attack.

39. For example, bitcoin miners are incentivized to perform the verification function through grants of new bitcoins. *See infra* note 114 and accompanying text. This creates a functional tax through inflation.

transaction costs.[40] Transaction costs need not be zero, merely low enough to open a range of new uses. The Internet, for all of its "free" price points, is extraordinarily expensive to maintain. Yet near-zero costs have produced a range of highly scaled and novel applications. For each drop in transaction costs, a new range of widely scaled and potentially disruptive uses becomes practicable.[41] Eliminating the cost of trust creates the possibility of true Internet-like scalability for property and currency transactions.[42]

Trustless ledgers can and will reshape property law if they push price points low enough to unleash disruptive and scalable applications. Property registries as they currently stand are a hodgepodge of relatively inaccurate, sometimes insecure, and often expensive ledgers.[43] Property records are notoriously costly to search.[44] Companies that maintain ledgers (and cannot perfectly price discriminate) have incentives to bar access to some potential users in order to keep prices high. Access fees to ledger databases are often well above what ordinary people can pay, and thus the systems do not scale. As two scholars, describing unsuccessful attempts to reform the land transfer system in 1939, lamented:

> Yet for the achievement of such reforms without payment of undue and continued tribute to private monopolies and without fruitless bother and delay—perhaps even if they are to be achieved at all—major changes must be effected in our antiquated, pre-commerce "system" of land transfer. Cheap, expeditious, and secure methods must be designed, if they are not already available, to replace the present complicated and dilatory methods which, while costly to the individual and burdensome to the public, afford no adequate security of title. Streamlined need cannot long endure horse-and-buggy obstacles to the liquidity of land. It is an ancient query, but its relevance grows: why should not a lot or a farm be as easily acquired and as securely held as a ship or a share of stock or an automobile?[45]

---

40. Werbach, *supra* note 22, at 347–48.

41. *See id.* at 349 ("Common networks facilitate innovation independent of the infrastructure platform, which can create significantly more value than the network itself.").

42. *See* Frankel, *supra* note 35, at 460 ("[I]f the risks and costs of reducing the risks to the *trusting* party are higher than the benefits, it will not interact. If the costs to the *trusted* party of establishing its trustworthiness are higher than the benefits, it will not interact.").

43. Myres S. McDougal & John W. Brabner-Smith, *Land Title Transfer: A Regression*, 48 YALE L.J. 1125, 1126–29 (1939) ("Why *cannot* a lot or a farm be so easily acquired and securely held? The answer can be found in any courthouse. It is in the wild disorder and the incompleteness of the public records.").

44. Peterson, *supra* note 1, at 1405.

45. McDougal & Brabner-Smith, *supra* note 43, at 1126 (footnotes omitted).

The problems of centralization, oligopoly, expense, and inaccuracy remain every bit as driving now as in 1939, and the central question remains unchanged: why should not numerous different forms of property be as easily acquired and as securely held as the simple switch of bits on a digital ledger?[46]

More is at stake than saving dollars on a few property transactions. Fixing property costs will change the Internet, not merely property law. A major use of the Internet is the transfer of property interests. Alibaba, eBay, and Amazon are prime examples.[47] The cost of property interest transfers operates as a component of, and thus a lower bound to, the efficiency of Internet technologies. Assuming consumers have different preferences and abilities to pay, there remains a range of transactions for which the minimum transaction cost outweighs the welfare surplus for the consumer or provider. These transactions do not occur because of cost, and the welfare gain is not realized. The costs of searching, moving, and maintaining interests in property act as a drag not only on individual actors seeking to transact at lower costs, but on the entire online ecosystem. By reducing the transaction costs associated with transferring property interests, it is possible to remove a serious limit on the ability of electronic applications to deliver welfare gains.[48] Minimum transaction costs enable microtransactions,[49] and microtransactions enable a range of wealth-generating behavior that is below the prior lower bounds of the property and currency systems. The lower the bound, the more new trades become possible; the smaller the transaction cost, the less wealth is simply left on the cutting room floor.

B. BITS AND BOLTS

This section provides a very brief overview of the mechanics of block chain technology, with a specific focus on new developments that make trustless public ledgers, such as the block chain, an interesting technology for property systems. The first subpart will deal with how trustless public

46. For the property initiate: this Article advances no position on the Torrens system itself, nor does that debate bear on this piece except to the extent of the motivating concerns of cost, convenience, and, in the context of Internet technologies, scalability.

47. *See generally What is eBay*, EBAY, http://pages.ebay.in/help/account/questions/about-ebay.html (last visited Mar. 26, 2015); *About Amazon*, AMAZON, http://www.amazon.com/Careers-Homepage/b?node=239364011 (last visited Mar. 26, 2015).

48. *See* Werbach, *supra* note 22, at 347–48 ("The internet fosters innovation by eliminating transaction costs, enabling new services to emerge.").

49. *Testimony of Jeremy Liew Before the New York State Department of Financial Services*, N.Y. STATE DEP'T FIN. SERVICES 1 (Jan. 28, 2014), http://dfs.ny.gov/about/hearings/vc_01282014/liew.pdf.

ledgers work, the second will explain how tokenized versions of existing public ledgers might be adapted to serve as public ledgers for property systems, and the third will deal with new developments in the technology that are particularly well-suited to property applications.

1. How Trustless Public Ledgers Work

a. The Double-Spending Problem

To create a coherent and useful online property system, one must solve the challenges of duplication and double spending.[50] Duplication is the first and most immediate problem.[51] If users can duplicate digital property, an MP3 for example, the marginal sale price commanded by the good goes rapidly to zero. Similarly, if a currency can be duplicated, the value of the currency evaporates under hyperinflation.

Double spending is a specific version of the duplication problem that emerges in systems that enact partially effective duplication controls.[52] Double spending occurs when the record owner of an asset conveys it forward to two (or more) different entities.[53] It is an exploit of the conveyance mechanism in property systems. Such systems must permit conveyance, but if conveyance can be from A to B, or from A to C, then A may seek to benefit from a conveyance to B and then to C, with neither B nor C knowing about the other.

Double spending becomes an issue whenever outright duplication has been made cost-prohibitive by some measure (say, license servers for MP3s, anti-forgery measures for land deeds, or anti-counterfeiting measures for currencies), and it becomes cheaper to exploit the conveyance

50. David Frisch, *Buyer Status Under the U.C.C.: A Suggested Temporal Definition*, 72 IOWA L. REV. 531, 531 (1987) ("The recognition of private property requires a comprehensive and systematic body of detailed rules to permit and control the transfer of property. Although these rules must necessarily comprehend innumerable transfer scenarios and force choices implicating difficult value judgments, at the most basic level two problems must be confronted: (1) how to accomplish a transfer of an item of property or an interest therein; and (2) how to resolve competing claims to the same item or interest.").

51. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 454 (1996) ("Because the digital cash is represented by a series of bits, and there are few things in this life easier to copy than bits, the bank is going to be very anxious to ensure that any copies of the digital cash . . . will be unspendable, or at least very easy to detect.").

52. *See* J.P. & G.T., *Virtual Currency: Bits and Bob*, ECONOMIST (June 13, 2011, 8:30 PM), http://www.economist.com/blogs/babbage/2011/06/virtual-currency ("This provides a degree of security against theft. But it does not prevent an owner of Bitcoins from spending his Bitcoins twice . . . .").

53. Kaplanov, *supra* note 5, at 117 n.35.

mechanism than to counterfeit the asset directly. For example, when counterfeiting dollars becomes hard and expensive, the petty crime of choice becomes writing bad checks. Check fraud exploits a delay in the currency conveyance system and enables the double spending of currency.

Double spending is a primary concern for both traditional property systems[54] and for cryptocurrencies.[55] It is easy to see why cryptocurrencies need to solve the double-spending problem. If one can spend the same currency multiple times, recipients cannot trust payments.[56] The creators of public ledgers expressly noted that their design was an attempt to solve the double-spending problem without resorting to centralized authorities.[57]

In this sense, the problems of public ledgers are the problems of property law generally. Prevention of double spending is just as much a central concern of traditional land conveyancing or personal property transfers as it is of digital property or cryptocurrencies.[58] Consider bona fide purchasers of land, for example.[59] A seller of land may convey land by multiple deeds to multiple downstream purchasers: basic double spending. The response of the law is a recording system, a ledger in which sales are recorded, to limit the potential for double sales.

Yet recording acts do not eliminate the problem because buyers do not have to record deeds in order for the transfer to be effective. Sellers can still exploit the conveyance mechanism.[60] So the law of conveyancing relies on incentives to encourage parties to get their interests on record by affording protection if the entry is recorded in the centralized ledger.[61] Depending on the state recording act, a subsequent bona fide purchaser of real estate, or a bona fide purchaser who files first, will take as against an

54. *See id.* at 117–18 ("In traditional payment systems, this problem is overcome by relying on a central authority to check each transaction or by issuing a serial number to prevent double spending.").

55. *See id.* at 116 ("[I]t may be difficult to prevent the same user from double spending the same digital coins by copying them.").

56. *Id.*

57. *Id.* at 116–17.

58. *See infra* notes 63–65 and accompanying text.

59. *See, e.g.*, Soulé v. Gragg (*In re* Harrison), 503 B.R. 835, 843 (Bankr. N.D. Okla. 2013) ("The rule is well established in [Oklahoma] that in the transfer of real estate in the absence of actual or constructive notice of a previous conveyance or of matters which would put a purchaser on inquiry, a bona fide purchaser for value will take good title to the property.").

60. *See, e.g.*, John W. Fisher, II, *The Scope of Title Examination in West Virginia: Can Reasonable Minds Differ?*, 98 W. VA. L. REV. 449, 455 (1996) ("Since recording first is not necessary to prevail against the 'earlier' unrecorded interest in a notice jurisdiction, the incentive to the subsequent bona fide purchaser to record promptly is to protect the title she or he acquired from 'another' subsequent purchaser.").

61. *Id.* at 454–56 (discussing past recording laws).

unfiled interest in the land.[62] This is a complicated and bad system for curtailing double spending. The risk falls on the purchasers (who often both have good faith) and does not directly reduce incentives to double spend in the first place. The risk can continue to spread if buyers further convey forward. A defect in title history can threaten downstream interests years and sometimes decades later.

In short, all property conveyance systems share problems of duplication and double spending. Until recently, there was only one broadly workable solution. A central, trusted authority or network of authorities was required to maintain the ledger and track, verify, and register all transactions.[63] For example, the Copyright Office verifies the integrity of the register of copyrights; the Patent and Trademark Office does the same for patents and trademarks; state Secretaries of State (for the most part) play this role under the UCC personal property filing system; and private entities like MERS and Depository Trust & Clearing Corporation fill similar roles for mortgages and stocks.[64]

Unsurprisingly, the first digital currencies followed a similar centralized model. A centralized issuing authority would maintain a trusted ledger on which transactions could be logged. DigiCash, eGold, and Venn are (or were) examples of digital currencies issued by central authorities.[65] Even those online digital currencies that were backed by some real commodity, such as gold or carbon credits, still relied on a central authority to maintain the register. Such registers were generally not public, and so trust in the issuer was an absolute necessity for the currency to gain widespread use. If trust in the issuer failed, for example, because the issuer inflated the currency by simply issuing more of it, or because of a failure to protect the ledger from hacks, the currency failed as well.

b. The Public Ledger Solution

A solution to the centralized authority problem was to make the ledger public. Imagine an online list intended to track ownership of property interests A, B, and C. At the start, perhaps Mary owns A, Joshua owns B,

62. *Id.*

63. *See* J.P. & G.T., *supra* note 52 ("In a centralised system, [theft is prevented] by clearing transactions through a single database.").

64. *See* Kaplanov, *supra* note 5, at 116 (describing the use of a distributed public ledger); *About Us*, U.S. PAT. & TRADEMARK OFF., http://wwwuspto.gov/about-us (last visited Mar. 27, 2015); *Overview of the Copyright Office*, U.S. COPYRIGHT OFF., http://www.copyright.gov/about (last visited Mar. 27, 2015).

65. *See* Middlebrook & Hughes, *supra* note 7, at 819–20 (describing a number of non-Bitcoin cryptocurrency and virtual currency implementations).

and Maggie owns C. We record this original set of interests in the list. Each time an interest changes hands, the ledger is updated, and the new list is distributed to everyone. In this way, the ownership interest can cheaply change hands with no need for a central authority.

Yet even with this extremely simplified system, there are several problems. Suppose Mary wishes to convey her interest to Grace. How can she do so, given that the two may not know each other, or may only be able to communicate electronically? The answer lies in cryptography.[66] Each person within the property system has a pair of cryptographically related keys, one public, given to everyone in the world to use, and one private, held only by the individual.[67] The keys are mathematically related, yet it is not possible to use the public key to guess the private key.[68] With the public key, one can send messages, bitcoins, or anything else, in a way that only the person with the private key can access. A commonly used analogy is that of a letterbox. The public key is the address of the letterbox. Anyone can put a letter in. But only the owner of the letterbox has the key to open it and retrieve the contents.[69]

Cryptography therefore secures the transfer of ownership interests in our simple online list. If Mary wishes to send her property interest to Grace, she encrypts it using Grace's public key and sends it. Only Grace can receive and decrypt it. Mary has confidence that she has sent the property to Grace, and Grace has confidence that no one else can access or use what was sent to her. The use of cryptography prevents anyone from standing in the middle of the transaction, since they cannot decrypt and therefore access the transmitted property interest. It does not prevent duplication or double spending, however. While Mary's ability to send the interest and receive payment is adequately protected by cryptography, there is the further problem that Mary may try to double sell her interest to both Grace and Hannah.

A log of transactions prevents double sales. If the log is up to date, a subsequent transfer from Mary to Hannah would be rejected because the record would show that Mary's interest had already been transferred to Grace. Trustless technology addresses the double-spending problem through the block chain, the decentralized and public log of all transactions.

66. *See* CHRISTOF PAAR & JAN PELZL, UNDERSTANDING CRYPTOGRAPHY: A TEXTBOOK FOR STUDENTS AND PRACTITIONERS 149–74 (2010) (discussing public-key cryptography).

67. J.P. & G.T., *supra* note 52. *See also Virtual Currency Schemes*, *supra* note 15, at 23 (describing public and private key pairing in a Bitcoin transaction).

68. Kaplanov, *supra* note 5, at 117.

69. BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 31–32 (1996).

For example, under the Bitcoin block chain protocol, transactions during a ten-minute period of time[70] are gathered by third parties (termed "miners" for reasons explored below) into a discrete "block" of transactions.[71] Once the transactions in a given block of time are verifiably baked into the overall list of transactions, they become the latest block of transactions in a chain of such blocks, hence the term block chain. The block chain constitutes a complete transaction history of all transfers of the asset (and, indeed, all other assets recorded in the chain), going back to the creation or original allocation of the asset.[72] All transactions must be registered with the chain and included in a block to transfer the interest.[73] Anyone can download the public ledger and thus see which keys hold which assets.

The significant innovation of the block chain lies in how blocks are added to the transactional chain without relying on a central authority, a process termed "mining." Miners are computers that provide computing resources to the network, and in turn, are rewarded through processing fees or through a grant of new bitcoins entering the system.[74] Miners do not discover new units—to that extent, the analogy to gold miners is misleading. Rather, miners do a lot of work to secure the system and are paid a small amount in a distributed fashion for their contributions.[75]

Mining consists of guessing numbers.[76] Imagine rolling a twenty-sided die. Each time someone rolls under a five, they get a reward. The more people roll, the faster results under five are generated; if that's happening too quickly, the system can adjust so that only rolls under a

70. J.P. & G.T., *supra* note 52. The time per block is arbitrarily set by the creators of the protocol, and the algorithm adjusts so that new blocks are opened at the same rate regardless of the computing resources available to the network. New protocols, such as Litecoin, benefit from faster block times, meaning that transactions clear more quickly. Ian Steadman, *Wary of Bitcoin? A Guide to Some Other Cryptocurrencies*, ARS TECHNICA (May 11, 2013, 6:51 AM), http://arstechnica.com/business/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies.

71. *Virtual Currency Schemes*, *supra* note 15, at 24–25.

72. Kaplanov, *supra* note 5, at 118.

73. *Id.*

74. This is payment of processing fees by inflation. As new bitcoins enter the system, all prior bitcoins decrease very mildly in value, to the benefit of the entity which receives the new coins. The Bitcoin network in particular addresses this concern by creating a hard cap of 21 million bitcoins that can ever exist and decreasing the rate of return in new bitcoins per block, so that eventually miners will be paid entirely from small processing fees rather than by inflation of the overall system. But this is essentially an advertising point for the system, which is meant to attract anti-inflationary monetary theorists. The system could just as easily be designed with a constant and limited inflationary rate to continue paying for mining through inflation. *Id.* at 119–21.

75. *Id.*

76. Thanks to Google engineer Mike Shick for providing this analogy in conversations at the Digital Asset Transfer Authority Gala, and for his continuing kindness in describing the underlying technology.

three or under a two are rewarded. This kind of dice rolling appears to be, and in fact is, a waste of resources. The dice rolling discovers nothing worth discovering. But the dice rolling has one advantage. If the only way to get a result is to roll, and if there is no way to simulate or falsify rolling, then people have to roll the dice to play the game.

This is how the block chain works.[77] Mining computers attempt to guess a hash value.[78] "A hash is a way of transforming an arbitrary amount of data to a fixed size number."[79]

> [Thus,] a hash is not invertible (you can't recover the data from the hash) and a small change in the input data creates a large change in the hash value. Miners search for hashes with particular characteristics (for example, the number of leading zeroes) in the only way possible: by taking the block and adding a random number to it, and then computing the hash of the block plus the random number, and checking it for the desired characteristics.[80]

The hash is unpredictable.[81] No one can tell ahead of time what the result of each try will be. The only way to do it is to guess repeatedly and rapidly. The protocol then sets a number of zeroes that must appear at the beginning of the resulting hash as a way of adjusting the problem difficulty. As more computers join the network, the math problem that must be solved to open a new block simply becomes more difficult. Of course, the analogy has limits. The so-called dice rolled in the Bitcoin protocol have more sides than there are atoms in the universe.[82] But for purposes of this discussion, the idea is that miners must roll dice until they get an arbitrarily difficult result.

Each time a miner finds a hash that meets the threshold, that miner is permitted to add a block to the chain. The miner has proven that it has done the work necessary to find a solution. Hence, the process of securing a block chain is called a "proof-of-work" system.[83] Each block's numerical value (unrelated to its financial value) is linked to the value of the prior block. In order to falsify the block chain, an attacker must do two difficult

77. *See* Kaplanov, *supra* note 5, at 118–19.

78. *Id.* at 118 n.49.

79. Thanks to Google engineer Nathaniel Fairfield for this analogy, suggested in comments to the piece and used with permission.

80. Kaplanov, *supra* note 5, at 118 n.49.

81. *Id*.

82. Alex Gorale, *Explaining the Math Behind Bitcoin*, CRYPTOCOINSNEWS (Oct. 18, 2014, 11:44 AM), http://www.cryptocoinsnews.com/explaining-the-math-behind-bitcoin/.

83. Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529, 532 (2014).

things. If the attacker wishes to change a past transaction, the attacker must—alone!—win enough die rolls so that she outpaces the rest of the system. That is, faking the past is prohibitively difficult because any attacker would have to match the combined processing power of the entire network over that period of time. And to continue the falsification moving forward into the future, the attacker would have to make guesses faster than the current block chain. The protocol accepts as true the block chain with the greater computational difficulty.[84] So an attacker would have to guess more hashes faster or at a higher computational difficulty than the rest of the currently functioning network.[85]

The result is a distributed public ledger of interests that is difficult to falsify and that becomes harder to falsify as more computers are added to the network. It would take hundreds of times the processing power of all of the world's top fifty supercomputers to accomplish that task. Keeping up the deception would be like lifting an ever-increasing stack of cars just to steal a hubcap. This new mix of security and decentralization is the reason that public ledger technology has received so much attention from entrepreneurs and innovators.

c. Network Effects and Vulnerabilities

The system is not without its vulnerabilities.[86] The ability of a trustless ledger to provide frictionless transactions is directly tied to its ability to scale. As Marc Andreessen noted:

> Bitcoin is a classic network effect, a positive feedback loop. The more people who use Bitcoin, the more valuable Bitcoin is for everyone who uses it, and the higher the incentive for the next user to start using the technology. Bitcoin shares this network effect property with the telephone system, the web, and popular Internet services like eBay and Facebook.[87]

84. Although this is often expressed as the network preferring the longer block chain, that is not always the case. Imagine a block chain made up of easier computational guesses—that chain could be longer in terms of blocks than a shorter chain comprised of much more difficult computational guesses.

85. *See* Kaplanov, *supra* note 5, at 120 n.57 (stating that an "attacker would require fifty percent of the processing power to disrupt the bitcoin network, an unlikely event"). More recent theories indicate that a 33 percent stake would be enough to disrupt the currency. Samuel Gibbs, *Bitcoin Could Be Hijacked by "Selfish" Groups Causing Currency Collapse*, GUARDIAN (Nov. 5, 2013, 7:26 AM), http://www.theguardian.com/technology/2013/nov/05/bitcoin-hijack-research-mining.

86. The means by which a trustless ledger might be compromised is beyond the scope of this piece. Broadly, centralization is the primary threat. If too much of a network is concentrated in the hands of any one group, then that group can subvert the network by brute force. It is also of course possible to compromise the security of the exchanges, but this is a matter of general cybersecurity.

87. Andreessen, *supra* note 6.

The network effect can propel a new technology to prominence and widespread adoption, but it can also impede innovation. Inferior technologies can defeat superior technologies by virtue of large and established networks. Thus, for example, the market in desktop operating systems is commonly held to have stagnated because of the large legacy network of installed operating systems. Only with the advent of tablet and smartphone operating systems was the installed base different enough to permit a new and competitive network to grow.

The problem with network effects and innovation often stems from the proprietary nature of the network. This is what prompts cries for antitrust enforcement against companies that occupy a dominant network position in an online market.[88] When monopolists lock out competitors, the threat to innovation is clear. However, the threat does not entirely, or even predominantly, arise out of anticompetitive urges. Even in a decentralized network, the value of the network grows non-linearly as a function of the number of nodes in the network.[89] Simply put, an innovator may need to build on top of an existing network, rather than start her own network, even if there is no anticompetitive entity seeking to lock her out.

As a result of this network effect, innovators will have great difficulty establishing their own completely separate networks.

> For this reason alone, new challengers to Bitcoin face a hard uphill battle. If something is to displace Bitcoin now, it will have to have sizable improvements and it will have to happen quickly. Otherwise, this network effect will carry Bitcoin to dominance.[90]

Just as the existence of strong network effects provides a challenge to innovators, innovators undermine already existing networks if they are forced to build separate networks rather than building on what is already available. For example, the attempt to establish separate block chains undermines the security of the main Bitcoin block chain. The more computers contribute processor cycles to the block chain by mining, the more secure it is. If mining resources are divided between two networks, both networks are weaker. Further, because security grows non-linearly as a function of the number of nodes, both networks are significantly weaker

88. *See generally* STAN J. LIEBOWITZ & STEPHEN E. MARGOLIS, WINNERS, LOSERS AND MICROSOFT: COMPETITION AND ANTITRUST IN HIGH TECHNOLOGY (1999) (analyzing the Microsoft antitrust case in the context of the high-speed software industry).

89. For example, Metcalfe's Law posits that the value of a communications network grows as the square of the number of nodes. *See* James Hendler & Jennifer Golbeck, *Metcalfe's Law, Web 2.0, and the Semantic Web*, 6 J. WEB SEMANTICS 14, 14 (2007).

90. Andreessen, *supra* note 6.

than one network with double the resources would be. Baby block chains are both a threat to the main block chain—since they take power that would otherwise be available to that system and divert it—and are themselves vulnerable, since they do not have the processing power to defend themselves.

This is the current state of affairs. The current main Bitcoin block chain resists falsification because it is the biggest network.[91] A large amount of processing power would need to be devoted to the block chain over a significant period of time in order to falsify the public ledger. New technologies and uses will be more secure if innovators can build them on top of the Bitcoin block chain rather than starting afresh and attempting to gather another network of computers. In a way, first adopters are the scarce resource. Getting enough miners to join a new network detracts from the prior network. If a full range of different and innovative applications could be built on top of the same block chain, then each technology could benefit from the strength and security of the combined mining for that chain. Technologies built on top of the current Bitcoin block chain would take shelter in the security of the current network, while being available for the development of new uses.

2. Tokenized Property

Innovators who wish to implement property systems in a trustless ledger might create their own network, separate from all others, and try to make that network large and fast.[92] They are likely to better succeed, however, if they build property systems on top of existing networks. One way to do so is by treating the slots in a public ledger not as coins, but as tokens that represent a property interest.

Consider, for example, a group that wished to tokenize rights in favors. So if A owes B a favor, B may wish to convey that favor to C, and C to D, and so on. If the group wanted to expand the favor network to the entire country, it could purchase a single bitcoin. Since bitcoins are divisible to eight decimal places, the group then could divide that single

91. However, falsification is feasible, especially during technological paradigm shifts. For example, the shift to application-specific integrated circuit mining led to a concentration of mining power within the Bitcoin ecosystem, such that one mining group was, for a twelve hour span, able to surpass the 51 percent mark. Joel Hruska, *One Bitcoin group now controls 51% of total mining power, threatening entire currency's safety*, EXTREMETECH (June 16, 2014, 10:43 AM), http://www.extremetech.com/extreme/184427-one-bitcoin-group-now-controls-51-of-total-mining-power-threatening-entire-currencys-safety.

92. *See* J.P. & G.T., *supra* note 52 (discussing how security in block chain technologies consumes processing cycles and requires widespread adoption).

coin up and issue one hundred million tokens—each one a single "satoshi," the smallest unit of bitcoin that can be tracked and traded.[93] A satoshi originating from the "favor" bitcoin would represent the favor. For a cost ranging between $500 and $1000, the group could secure one hundred million tokens that are tracked and protected by the full computing power of the block chain.

There are efforts underway to build such systems on top of the Bitcoin block chain.[94] For example, a company might decide to convey ownership of a commodity like gold by tying it to specific coins within the chain.[95] The company may then arbitrarily designate coins that it owns as "colored," that is, as having some significance beyond the coin itself.[96] This designation in no way impacts the rest of the block chain, which is in fact oblivious to the additional meaning attached to the coins by the company. Any coin traceable back to an original gold-colored coin takes on the characteristics of the original coin. Whoever controls the coin, controls the commodity. Multiple colors are of course possible, with each different application resting on a different set of colored coins.

The more closely the conveyed interest is tied to the token, the more effective token systems become. For example, assume that the interest parties wished to convey was the ownership of the token itself. The public ledger would accomplish that without any complexity. The person who has the token in their digital wallet—that is, the person to whom the ledger ascribes ownership—would hold the right.

There is only slight additional complexity for tracking intangible rights distinct from, but connected to, the token. Consider a fantasy baseball league in which participants trade "players" by ascribing to one person within the league the right to use a particular real-world player's stats in determining the success of a virtual baseball team. Only one participant within the league may count a player on their virtual team, per the rules of the game. The resource is separate from the token. The token is not the resource itself, but the token conveys the right in a public fashion, so that participants in the system may know who may exercise the right.

Tying a token to a legal right is common in property law. For

93. Andreessen, *supra* note 6; Jim Kessler, John Vahey & Matthew Caulfield, *Bitcoin: Back to the Future*, THIRD WAY (Jan. 16, 2015), http://thirdway.org/report/bitcoin-back-to-the-future.

94. *See, e.g.*, Ethereum, *Vitalik Buterin Reveals Ethereum at Bitcoin Miami 2014*, YOUTUBE (Feb. 1, 2014), http://www.youtube.com/watch?v=l9dpjN3Mwps (discussing various uses for the Bitcoin block chain).

95. *Id.* at 4:35.

96. *Id.* at 5:05, 8:20.

example, while land itself cannot be conveyed in a ledger, it is legally uncontroversial to tie the right to land to a token—a deed[97]—that can be cheaply and quickly transferred, and that can be recorded in a ledger of interests. If there is a dispute as to the ownership of a plot of land, courts refer to the land records ledger, at least as a starting point.[98] To give another example, a stock certificate has no intrinsic value. The certificate serves as a token that conveys certain rights; for example, the right to vote or the right to receive dividends. From handing over the car keys as symbolic delivery of a gift of personal property,[99] to conveying ownership in bulk commodities through warehouse receipts,[100] to the ritual of livery of seisin at common law, the law has long recognized the need to transfer property interests through the expedient of a symbol, deed, or token.[101]

Token systems work well to transfer rival legal rights to exercise the prerogatives of ownership over a given resource, whether in the form of a stock certificate, oil or gas lease, land deed, copyright or patent registration, or any other right dependent on a ledger entry. The question is not whether those rights can be tokenized. They already are. The relevant question is whether a trustless, public, and cryptographically secure ledger can provide better tokens. Currently extant property transfer systems were originally adopted because they offered better security, more certainty, and lower costs than prior methods of property conveyance. In the same way, new systems that improve security, certainty, and speed at reduced cost have the potential to improve on legacy property systems.

Tokenized public ledgers offer new solutions to old property problems. The tokens can be securely transferred for very little cost. A

97. Carol M. Rose, *Introduction: Property and Language, or, the Ghost of the Fifth Panel*, 18 YALE J.L. & HUMAN. 1, 20 (2006).

98. Milner v. Milner, 361 S.W. 3d 615, 621 (Tex. 2012) ("Record title . . . typically refers to legal evidence of a person's ownership right in property."). *Compare* United States v. Ellis, 739 F.2d 1250, 1254 (7th Cir. 1984) ("Illinois law defines the owner of an automobile as the person holding title . . . ."), *and* Tusa v. Omaha Auto Auction, Inc., 712 F.2d 1248, 1251 (8th Cir. 1983) ("[T]he Nebraska Supreme Court held that there would not be an exception to the general rule that the title is conclusive evidence of ownership where the titleholders voluntarily put their names on the title . . . ."), *with In re* James, 496 B.R. 590, 595 (Bankr. W.D. Ark. 2013) ("[I]n Arkansas, certificate of title is only evidence of title to a vehicle, not title itself.").

99. *See* RESTATEMENT (THIRD) OF PROP.: WILLS & OTHER DONATIVE TRANSFERS § 6.2, cmt. g (2003) (discussing symbolic delivery). Possession is used as the crudest proxy of all, but *faute de mieux* has remained in widespread use. Willcox v. Stroup, 467 F.3d 409, 412 (4th Cir. 2006).

100. Donald B. Pedersen, *Electronic Data Interchange as Documents of Title for Fungible Agricultural Commodities*, 31 IDAHO L. REV. 719, 732–36 (1995).

101. *See* Frisch, *supra* note 50, at 531 ("To deal with the [problem of competing interests in property], one finds a history rich in rules clothed in ceremonial garb. The play is everything: a transfer occurs only if properly performed.").

block chain can trace transactions even where the number and speed of such transactions would confound a regular recording system.[102] Attempts to double spend tokens are rapidly detected and resolved. Unlike many property systems, where clouds on title resulting from double spending can last for years, double sales within a public ledger are blocked within minutes. Indeed, while the passage of time makes interests in traditional property more obscure and less secure, the passage of even an hour builds a transaction so firmly into the block chain that it cannot practically be reversed or falsified.

3. Protocol Networks and Side-Chains

Enthusiasts and entrepreneurs have proposed a range of improvements to public ledger technologies.[103] Some of the best ideas address how the protocol can support uses beyond simple currency simulation. Thus, for example, one innovative proposal is to use the block chain as a communications protocol on top of which anything can be built, rather than merely a currency with some alternative uses through tokenization. This approach uses a Turing-complete programming language to permit users to create any program, riding on top of a decentralized block chain, rather than riding on top of a traditional database.[104] The functional entity within the proposed new system is a "contract"—a software agent that resides within the block chain and commands resources from that chain.[105] For example, parties might set up a very simple hedging contract, in which both parties put one thousand dollars' worth of trustless currency in, and the hedging party would, at the end of the contract, receive one thousand dollars' worth of currency back, hedging the risk against downward market volatility but granting upside gains to the other party.[106]

Networks built to service a range of applications offer significant advantages over networks built for a single use case. For example, treating the block chain as a communications protocol would open trustless public ledgers to more advanced property applications. It may well be that the existing main block chain needs to be reworked in order to serve as an effective underlying protocol for the broader range of applications that startups are now considering. Yet there is a cost each time for doing so, and

102. *See Virtual Currency Schemes*, *supra* note 15, at 21 n.4 ("[A]ll Bitcoin transactions are recorded and can . . . be traced.").

103. *See generally* Ethereum, *supra* note 94 (discussing various implementations for the Bitcoin block chain).

104. *Id.* at 9:15.

105. *Id.* at 6:28.

106. *Id.* at 6:46.

it is entirely possible that at some point, the network benefits of an existing public ledger will be sufficiently high that starting over is not an option. In short, there must be another way to innovate in public ledger technology besides starting the network over each time.

Another innovation, called a "side-chain," may make it possible to leverage the strongest existing public ledger for new and innovative applications, without requiring those technologies to start over and build entirely new networks.[107] In a side-chain, the creators of an innovative technology root a new block chain in the main Bitcoin block chain through Bitcoin contracts, which permit the automated exchange of the sidechain currency back into the main block chain.

Consider a company that wishes to develop a new, faster block chain. The company cannot merely create tokens based on the main Bitcoin block chain, since those new transactions will only be processed at the speed of the main chain—one block every ten minutes. Instead, the company might create a new and faster block chain, but one that is grounded in and convertible to the main block chain through preprogrammed Bitcoin contracts. If the new currency flops because, for example, the innovation is not attractive to users, then those users who did invest in the alternative currency can convert their holdings back into Bitcoins on the main block chain. Side-chains therefore significantly reduce the cost of innovation.

Tokenizations and side-chains each offer the possibility of building a large range of applications on top of a single, powerful block chain. While diverse applications built on the same network spur growth and innovation, the multiplicity of interconnected use cases presents a serious problem for regulators. The following section discusses a number of the different emerging use cases for block chain technologies, as well as some of the currently developing regulatory responses.

C. USE CASES AND REGULATORY REGIMES

The regulatory framework that will govern trustless public ledgers is a function of the narrative surrounding them. Technologies are created by narratives, and they are regulated by narratives.[108] Bitcoin is as much

107. Jon Evans, *Bitcoin 2.0: Unleash the Sidechains*, TECHCRUNCH (Apr. 19, 2014), http://techcrunch.com/2014/04/19/bitcoin-2-0-unleash-the-sidechains.

108. *See* DAVID E. NYE, AMERICA AS SECOND CREATION: TECHNOLOGY AND NARRATIVES OF NEW BEGINNINGS 4–11 (2013) (detailing America's "technological foundation story"); Steven Wilf, *The Making of the Post-War Paradigm in American Intellectual Property Law*, 31 COLUM. J.L. & ARTS 139, 175–76 (2008) (revealing the conflict between two narratives of intellectual property's industrial pluralism in the New Deal); Robert P. Merges, *Software and Patent Scope: A Report from the Middle*

driven by a social narrative as it is by innovative technology.[109] That narrative springs from a driving need for online global currency, from a sense of technological optimism, and from the still-vibrant story that groups can solve their own problems, given low enough transaction costs.[110] This narrative has fueled a range of powerful alternatives to traditional and costly financial structures and payment networks.[111] Conversely, the narrative of criminal uses for online currencies has fueled the regulatory push that has overtaken them.[112]

Cryptocurrencies can be used to transfer value, even if they are not currency per se.[113] Because of this, regulators are currently examining Bitcoin and like cryptocurrencies almost purely from the perspective of financial services regulation.[114] The danger is that this could imperil innovations built on top of the block chain that do not fit a financial services model.[115]

While the financial narrative is well established online, the property narrative has a much more tenuous foothold. The technological tools are already in place to push trustless technologies well beyond their cryptocurrency implementation. The current need is for a legal and social narrative that can, when combined with extant technology, provoke similar development and innovation in other value-transfer systems.

Innings, 85 TEX. L. REV. 1627, 1645 (2007) ("For [American jurists], patents were not a vestige of corrupt political maneuvering, but instead represented the flourishing of a vital, energetic young nation."); Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management*,*"* 97 MICH. L. REV. 462, 561 (1998) (discussing how one narrative of DRM technology may have limited innovation in the field); Gregory S. Alexander, *Takings, Narratives, and Power*, 88 COLUM. L. REV. 1752, 1752–53 (1988) (examining the narrative behind regulatory takings).

109. David Groshoff, *Kickstarter My Heart: Extraordinary Popular Delusions and the Madness of Crowdfunding Constraints and Bitcoin Bubbles*, 5 WM. & MARY BUS. L. REV. 489, 511–22 (2014).

110. Sarah Jeong, *The Bitcoin Protocol as Law, and the Politics of a Stateless Currency*, SSRN 1 (May 8, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124 (stating that the creators of Bitcoin believed that "currency and economic activity can arise spontaneously without centralized authority . . . .").

111. *See, e.g.*, Groshoff, *supra* note 109, at 509–10 (describing one of the first virtual currencies, DigiCash, and the impact its failure had on cryptocurrencies).

112. *See* Kaplanov, *supra* note 5, at 167–69 (discussing the current push for regulation of Bitcoin).

113. *See* Farmer, *supra* note 7, at 104 (arguing that Bitcoin should not be classified as a currency or security, but as "something new").

114. *See* Middlebrook & Hughes, *supra* note 7, at 814–20 (discussing various federal and state actions addressing Bitcoin and other cryptocurrencies); *Virtual Currency Schemes*, *supra* note 15, at 13–18, 33–45 (creating a categorization scheme for virtual currencies and describing the emerging European regulatory framework for such currencies, including the potential applicability of a range of European financial services laws).

115. *See* Farmer, *supra* note 7, at 104 (arguing that treating Bitcoin as either a currency or security will cause problems).

It is worth briefly examining the emerging regulatory framework surrounding cryptocurrencies for two reasons. First, it is useful to get a sense as to how the features of a given use case drive the regulatory response. Second, the financial regulatory response is very likely to become tangled with new, non-currency use cases for public ledgers as they emerge. This section explores the ways in which cryptocurrency and alternative use cases have become tangled as a matter of regulatory focus. The following subparts look first at the regulatory regime currently governing trustless system architectures before turning to a discussion of the property use cases that trustless public ledgers enable.

1. Currency and Payments

Currency, or a substitute thereof,[116] is the most prominent current use case for trustless architectures. The Internet has long needed something that can serve as a decentralized unit of account, store of value, and medium of exchange. Trustless public ledgers work well as currency substitutes because conveyance of the ledger entry is a transfer of the asset itself. In currency systems, the transferor is not trying to transfer something else by using the unit of cryptocurrency as a symbol for that other thing. The transferor merely transfers the unit by transferring the ledger entry.[117] A trustless public ledger serves that purpose simply and admirably.

Cryptocurrency also answers a market need for online cash equivalents. Cryptocurrencies improve on the traditional system of cash, checks, and cards. Traditional currencies are not sufficiently divisible so as to enable the kind of micropayments necessary for many Internet transactions,[118] and the transfer networks for cash through the financial system are too expensive for transactions of only a few cents to be worth transferring.[119] Cryptocurrencies enable long-distance, low-trust, and low-cost microtransactions.

Regulators have chosen to regulate cryptocurrency businesses under the payments regulatory framework. This is because, in addition to serving as a currency substitute, ledgers also serve as payment systems: a method of settling debts and transferring value from one person to another. Thus,

116. The terms "currency substitute" and "cryptocurrency" are used to denote the fact that while cryptocurrencies are not currencies or money as defined by law, they are still captured under a range of statutes that regulate transmission of value. *See infra* Part I.C.1.a.

117. *See* J.P. & G.T., *supra* note 52 (describing how bitcoins are transferred).

118. For example, microtransactions are a common means of selling high volumes of low-dollar-value digital items in video games or social networks.

119. Grinberg, *supra* note 7, at 170.

the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") has spearheaded regulatory efforts surrounding cryptocurrencies. FinCEN has the authority to regulate money services businesses ("MSBs") and issue implementing regulations under the Bank Secrecy Act.[120] FinCEN's approach has been to deem cryptocurrencies a kind of "value that substitutes for currency," such that businesses conducting transfers using cryptocurrency may be drawn into the definition of a regulated MSB under the Act.[121]

Under FinCEN regulations, an MSB is a non-bank, non-depository institution that engages in one of an enumerated list of financial services, from check cashing to issuing prepaid access.[122] MSBs do not include banks, businesses regulated by the Securities and Exchange Commission or the Commodity Futures Trading Commission, or any person who engages in one of the enumerated financial services "on an infrequent basis and not for gain or profit."[123] Perhaps the broadest sub-category of MSBs is that of money transmitters.[124] This category includes entities that engage in "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means,"[125] or even more loosely, "[a]ny other person engaged in the transfer of funds."[126]

120. Currency and Foreign Transactions Reporting (Bank Secrecy) Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951–1959, 31 U.S.C. §§ 5311–5322 (2012)) (granting the Department of the Treasury the power to implement regulations under this act); 31 U.S.C. § 310(a) (establishing FinCEN as a bureau within the Department of the Treasury); Treas. Order 180-01 (July 1, 2004), *available at* http://www.treasury.gov/about/role-of-treasury/orders-directives/Pages/to180-01.aspx (delegating enforcement of the Bank Secrecy Act to FinCEN); *FinCEN's Mandate from Congress*, FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/statutes_regs/bsa/ (last visited Mar. 29, 2015).

121. The hook to virtual currencies lies in the inclusion of "other value that substitutes for currency" within the FinCEN regulations. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2012).

122. *Id.* § 1010.100(ff).

123. *Id.* §§ 1010.100(ff)(8)(i)–(iii).

124. *Id.* § 1010.100(ff)(5).

125. *Id.* § 1010.100(ff)(5)(i)(A).

126. *Id.* § 1010.100(ff)(5)(i)(B). Typical of complex and repeatedly amended statutory schemes, additional and potentially conflicting mentions of money transmission appear elsewhere in the Code. For example, for purposes of determining which entities must register with the Secretary of the Treasury, 31 U.S.C. § 5330 (2012) defines a "money transmitting business" as "any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system," and that is not a depositary institution, which is required to file reports under 31 U.S.C. § 5313. That statute in turn provides guidelines for reporting domestic coin and currency transactions. 31 U.S.C. § 5313.

An MSB must comply with a range of registration, record-keeping, and reporting requirements, including know-your-customer obligations and suspicious financial activity reporting.[127] An entity that fails to do so faces regulatory sanctions, as well as potential criminal liability under 18 U.S.C. § 1960 for the operation of an "unlicensed money transmitting business."[128] Section 1960 defines an unlicensed money transmitting business to include "a money transmitting business which affects interstate or foreign commerce in any manner or degree and . . . otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."[129] The statute provides for fines and imprisonment for up to five years.[130]

The definitions of "money transmitting business,"[131] "money transmitter,"[132] and "unlicensed money transmitting business"[133] in the regulations and criminal statute have created a regulatory thicket that has caught multiple issuers of online currency. *United States v. e-Gold, Ltd.*[134] considered whether the issuer of an online currency operated an unlicensed money transmitting business despite the fact that it did not deal in state-backed currency.[135] The court held that the definition of "money transmitting business" in 18 U.S.C. § 1960 (the criminal statute) was substantially broader than that found under the Bank Secrecy Act or its implementing regulations, and as a result, held that any unlicensed transmission of money on behalf of the public "by any and all means" was a criminal act.[136] Thus, for example, in May 2013, the founder and operators of electronic currency system Liberty Reserve were indicted on money laundering and unlicensed money transmission charges for operating an online virtual currency network heavily used by criminal organizations.[137] The breadth of application of 18 U.S.C. § 1960 seems only limited by the idea that an entity must engage in money transmission

127. *Id.* § 5330.

128. 18 U.S.C. § 1960(b)(1).

129. *Id.* §§ 1960(b)(1)(a)–(c).

130. *Id.* § 1960(a).

131. 31 U.S.C. § 5330(a)(1).

132. 31 C.F.R. §§ 1010.100(ff)(5)(i)(A)–(B) (2012).

133. 18 U.S.C. § 1960(a).

134. United States v. e-Gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. 2008).

135. *Id.* at 88.

136. *Id.* at 90. *See also* Middlebrook & Hughes, *supra* note 7, at 822–28 (analyzing the *e-Gold* prosecution and its implications for subsequent cryptocurrencies).

137. Sealed Indictment ¶¶ 30–32, United States v. Liberty Reserve S.A., No. 13 Cr. 368 (S.D.N.Y. May 28, 2013); Kim Zetter, *Liberty Reserve Founder Indicted on $6 Billion Money-Laundering Charges*, WIRED (May 28, 2013, 12:53 PM), http://www.wired.com/2013/05/liberty-reserve-indicted/.

as a business, or at least in more than an isolated fashion. For example, the *e-Gold* court noted: "Section 1960 was designed to tackle large-scale operations as opposed to small-scale or individual money transmitters."[138] Or, as the court in *United States v. Velastegui*[139] noted, "section 1960(a) requires that the unlicensed entity be 'an illegal money transmitting *business*' . . . which insures that persons or entities cannot be prosecuted for a single, isolated transmission of money."[140]

It was against this backdrop that FinCEN issued guidance in mid-2013 that defined the application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies, with the goal of clarifying when businesses or individuals would be subject to regulation.[141] That guidance differentiates between "users," "administrators," and "exchangers" for purposes of determining who must comply with the Bank Secrecy Act provisions falling under FinCEN's ambit. An "administrator" is an entity that issues or controls a virtual currency. A "user" under the guidance is "a person that obtains virtual currency to purchase goods or services."[142] An "exchanger" is "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency."[143] Despite FinCEN's efforts to clarify, there remains significant confusion regarding which entities are users and which are exchangers. In a trade, one person gives, and the other receives. Thus, for example, a "user" can generally only "obtain virtual currency," as defined by the guidance, through the "exchange of virtual currency for real currency, funds, or other currency"—the very definition of an exchanger.[144] As a result of this confusion, many startups are uncertain whether they must seek licensing as money transmitters, and many individual users are worried that they may be subject to sanction.

2. Property

Thus far, this section has addressed the regulation of cryptocurrencies as a payment rail. The technology is not limited to use as a payment system, however. Trustless public ledgers are value transfer systems, part

138. *e-Gold*, 550 F. Supp. 2d at 90.

139. United States v. Velastegui, 199 F.3d 590 (2d Cir. 1999).

140. *Id.* at 595 n.4 (alteration in original) (quoting 18 U.S.C. § 1960(a) (2012)).

141. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, DEP'T OF THE TREASURY FIN. CRIMES ENFORCEMENT NETWORK 1 (Mar. 18, 2013), http:// fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

142. *Id.* at 2–3.

143. *Id.* at 2.

144. *Id.*

of what commenters call the "Internet of Value."[145] Block chains can facilitate the transfer of more than mere coins. Trustless technology can disintermediate any system that ties an identity to a resource by making transfers of the resource to new identities reasonably secure, public, and low-cost. This makes it an intriguing technology upon which to base property registries. To date, however, property and commodity conceptions of block chain technologies are undertheorized and incomplete.

The costs of getting property theory wrong are significant. Clean property rules should reduce information costs. Unfortunately, the Internal Revenue Service's ("IRS") attempt to treat virtual currency as property for tax purposes does not. In 2014, the IRS published a notice regarding tax treatment of cryptocurrencies.[146] Those rules grew out of the IRS's prior experience with virtual assets in games and social networks, especially game currency or social network currency.[147] Such assets could be used or traded for other digital assets within a virtual environment.[148] Thus, for example, one might use the virtual gold in an online world to buy a coveted item or piece of virtual real estate. In a social network, a user might be willing to pay a small amount to decorate a social network page, or to send a small gift to a friend through the network.[149]

The first virtual currencies were initially restricted in scope precisely because their value was grounded in a specific environment.[150] One could only use virtual gold to buy items or assets in the virtual world that generated them.[151] Yet by the very fact that those currencies commanded assets that people deeply desired, the value of the currencies began to spread beyond the virtual worlds or social networks in which they originated.[152] Just as dollars are used in transactions entirely outside of the

145. Stan Higgins, *Money 20/20 Day 2: Automated Economies and the Internet of Value*, COINDESK (Nov. 4, 2014, 6:46 PM), http://www.coindesk.com/money2020-day-two-2014/.

146. I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (Mar. 25, 2014), *available at* http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

147. *See Virtual Currency Schemes*, *supra* note 15, at 11 ("In connection with the high penetration of the internet, there has also been a proliferation of virtual communities in recent years. . . . In some cases, these virtual communities have created and circulated their own digital currency for exchanging the goods and services they offer, thereby creating a new form of digital money . . . .").

148. *See, e.g.*, *id.* at 14–15 (describing virtual currencies in Facebook and Second Life).

149. *Id.*

150. For example, WebMoney, e-Gold, Pecunix, and Liberty Reserve are digital currencies that are based on or backed by the price of gold. *See generally* Peter C. Tucker, *The Digital Currency Doppelganger: Regulatory Challenge or Harbinger of the New Economy?*, 17 CARDOZO J. INT'L & COMP. L. 589 (2009).

151. Leah Shen, *Who Owns the Virtual Items?*, 2010 DUKE L. & TECH. REV. 1, 1–2 (2010).

152. Peter M. J. Gross, *A History of Virtual Currency: Why Bitcoins Shouldn't Surprise You*, CFA INST. (Jan. 10, 2014), http://annual.cfainstitute.org/2014/01/10/a-history-of-virtual-currency-why-

United States, virtual currencies also began to command value outside of their worlds or networks of origin. Chinese citizens began using Q-coins, a social network currency, to purchase everyday goods and services.[153] Players of multi-million-player online games began to start businesses in which they generated virtual gold not to play the games, but for the purpose of selling the gold for dollars.[154]

As early as 2007, the IRS was aware of the potential for tax avoidance through virtual property and virtual currencies.[155] If virtual assets could be converted to real dollars and back, then ordinary assets could be hidden in virtual worlds and payments could be made without showing any gain in income. The critical question was how to treat virtual assets that might be used purely for play purposes, but which also could be easily sold to other players to turn a profit.[156]

This tension caused the IRS to hesitate to issue formal guidance. The IRS settled instead in 2009 on an informal cash-out rule that looked something like the rules for realization of gain upon disposition of property, or capital gains.[157] If the digital property merely increased in value within the virtual environment, no tax liability accrued. As such, when users increased their virtual holdings, or their virtual holdings otherwise increased in value, they incurred no tax liability. If, however, users exchanged virtual assets for dollars, they were liable for the income generated as a result. This system protected the broad range of users who were simply playing games or purchasing assets within online communities, as users who kept their assets and transactions virtual paid no tax. This was not a significant concern because almost all such assets needed to be exchanged for dollars before purchasing other assets.

bitcoins-shouldnt-surprise-you/.

153. *Central Bank Threatens to Step into "Virtual Money" Controversy*, XINHUA NEWS AGENCY (Nov. 16, 2006, 10:35 AM), http://news.xinhuanet.com/english/2006-11/16/content_5337155.htm (discussing Q-coin use in China).

154. Richard Scott, *The Business End of Playing Games*, BBC NEWS (Apr. 25, 2007, 2:55 PM), http://news.bbc.co.uk/2/hi/technology/6592335.stm.

155. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-516, VIRTUAL CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX COMPLIANCE RISKS 15 (2013) [hereinafter GAO VEC REPORT].

156. *See* Bryan T. Camp, *The Play's the Thing: A Theory of Taxing Virtual Worlds*, 59 HASTINGS L.J. 1, 2 (2007) (arguing that only those who convert virtual items to cash should be taxed on that income); Leandra Lederman, *"Stranger than Fiction:" Taxing Virtual Worlds*, 82 N.Y.U. L. REV. 1620, 1622–24 (2007) (discussing whether receiving online game items should be taxed when only some users sell them for profit); Jacqui Cheng, *The Taxman Cometh? IRS Urged to Tax Virtual Worlds, Economies*, ARS TECHNICA (Jan. 12, 2009, 11:04 AM), http://arstechnica.com/gaming/2009/2009/01/taxpayer-advocate-urges-irs-to-tax-economy-in-virtual-worlds/.

157. GAO VEC REPORT, *supra* note 155, at 1–2.

The tenor of the conversation shifted as virtual currencies outgrew their origin in games, virtual worlds, and social networks. In 2013, the Government Accountability Office ("GAO") issued a report to the Senate Committee on Finance on potential tax treatment for virtual economies and currencies.[158] The GAO report detailed how the IRS could address tax treatment of currencies and assets obtained and used within virtual worlds, social networks, or games.[159] The report noted that while some economies used virtual currencies "as a medium of exchange for goods and services" within an online environment, such assets "can have economic value outside of virtual economies" when traded for dollars.[160] Moreover, the report noted more recent currencies that "have been developed outside of virtual economies as alternatives to government-issued currencies."[161]

Following the GAO report, the IRS issued guidance determining that "[f]or federal tax purposes, virtual currency is treated as property,"[162] and as a result, "[g]eneral tax principles applicable to property transactions apply."[163] Yet unlike in the game context, where quasi-property treatment protected most users who never cashed out from tax liability, the IRS's inelegant election to treat cryptocurrency as property raises transaction and information costs. With each exchange of currency, the user must calculate gain or loss based on the rise and fall of the cryptocurrency against the dollar. Not only must a taxpayer who receives virtual currency as payment include it in computing gross income, but the taxpayer must also calculate the gain or loss upon exchange of virtual currency for other property.[164]

The IRS's property characterization directly impacts Bitcoin's use as a medium of exchange.[165] Based on the guidance, Bitcoin is taxed based on the market rise or fall in its value during the period of time that the owner held it.[166] If the going rate for a Bitcoin was $500 per coin when a consumer received .01 of a coin in the morning, and $750 per coin when that consumer used that same amount to buy a sandwich and drink at lunch, she would have realized $2.50 worth of taxable gain in the intervening hour. Treating convertible virtual currency as undifferentiated personal

158. *Id.* at 1.
159. *Id.* at 1–2.
160. *Id.* at 1.
161. *Id.*
162. I.R.S. Notice 2014-21, *supra* note 146.
163. *Id.*
164. *Id.*
165. *Id.*
166. *See id.* ("If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain.").

property poses a non-trivial threat to the use of the currency at the low end of the microtransactions scale. The requirement to calculate base value and gain on every receipt and expenditure made using convertible virtual currency significantly raises transaction costs.[167]

In sum, new technology raises the possibility for near-frictionless and reasonably secure disintermediated property exchange. But careful theory is needed if the benefits of these systems and their successor technologies are to be realized. The risk is that inelegantly conceived property systems will complicate trades by raising information costs. The following part therefore draws heavily on the established literature of information cost theory in property to develop a framework for understanding the role of good property rules in reducing information costs, and the proper design parameters for digital property systems in light of that role.

II. BITPROPERTY

The preceding part discussed digital systems that might significantly improve upon current methods of tracking and transferring property interests. This part starts a conversation about the future of property. In doing so, it seeks to address the mystery of digital property: why do we truly own so little online? Why has traditional (i.e., non-intellectual) property law failed to gain a real foothold in digital environments? What conceptual blocks remain in place, preventing the full adoption of online property regimes? And what can be done within the realm of theory to begin to shift the conversation?

The core common law areas have taken markedly different paths in their transition to online environments. Contract law has made an effortless transition to the Internet.[168] Electronic contracts are everywhere and routinely enforced. Tort law has made a similarly seamless transition.[169] Cyberdefamation is a routine cause of action, and specific online issues like cyberbullying or revenge porn are hotly discussed topics, where progress in the debate can be discerned.[170]

167. *See* Kashmir Hill, *How I Paid My Bitcoin Taxes*, FORBES (Apr. 15, 2014, 2:26 PM), http://www.forbes.com/sites/kashmirhill/2014/04/15/how-i-paid-my-bitcoin-taxes/ (discussing the burdens of recordkeeping for Bitcoin transactions).

168. Rachel S. Conklin, *Be Careful What You Click for: An Analysis of Online Contracting*, 20 LOY. CONSUMER L. REV. 325, 329–30 (2008).

169. *See* Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 344–49 (2005) ("Instituting website liability for illegal postings has the potential to jumpstart the field of cybertorts so that it can develop into an effective social control mechanism for cyberspace.").

170. *See* Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 BERKELEY TECH. L.J. 55, 93–94 (2012) [hereinafter Fairfield, *Mixed Reality*] ("Such

Yet traditional property law has struggled to find secure footing online.[171] Traditional property, a system designed through a long tradition of common-law deliberation to govern interests in scarce and rival resources, did not seem at the time of the rise of the Internet to be immediately applicable to an environment in which many resources were neither scarce nor rival. At that time, the critical application of Internet technologies seemed to be unlimited duplication of non-scarce and non-rival information, rather than the frictionless transfer of scarce and rival resources. As a result, intellectual property, the law governing non-rival resources, became the dominant structure for online assets. Yet this structure is enormously inefficient for those who prefer to own rather than license.

For example, a consumer who purchases CDs owns the CDs but does not own the MP3s of the same music. Consumers do not own the e-books they purchase from Amazon Kindle, even though they would own the same books purchased in physical form. Property rights in physical copies of copyrighted material are utterly non-controversial. Property rights in digital copies of copyrighted material drift in a limbo of digital rights management technologies ("DRM") and end user license agreements.[172] No one can accuse intellectual property of being under-examined. Not so with the law of digital, rival property.

Traditional property law has long leveraged the physicality of assets as a proxy for the rivalrousness that buyers and sellers demand in property systems. The reason that one owns a table rather than purely licensing it from its creator is that the table's physicality makes it (for the most part) rival. It is easier to buy a table from someone than to duplicate it through copying. But, while physicality has been a proxy for necessary rivalrousness, it is only a proxy. What is necessary is that property be rival, not that property be physical. Ledgers provide the necessary rivalrousness with no requirement of physicality. Yet the rough dividing line between property and intellectual property law remains the false boundary of physicality.

reputational harms can already be found in the purely online context.").

171. *See* Elizabeth Townsend Gard & Rachel Goda, *The Fizzy Experiment:* Second Life*, Virtual Property and a 1L Property Course*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 915, 931–34 (2008) (discussing an example of the struggle to apply traditional property law to the online digital environment).

172. *See* Fairfield, *Mixed Reality*, *supra* note 170, at 100–01 (explaining that there is a trend towards corporate control, which increases the risk that "'virtual' rights holders (IP owners) will prevail and that 'real' rights holders (real people and owners of physical property) will lose out").

There have been previous attempts at creating theory bridging the physicality divide in property law, but these approaches have not fared well. For example, the specific literature on cyberproperty attempted to tie online property rights to offline chattel property rather than create digital assets that are rivalrous in their own right.[173] Under cyberproperty theory, if I can legally prevent someone from entering my house or interfering with my use of my car, I ought to be able to exclude someone from the physical property consisting of my computer server. By extension, therefore, the cyberproperty literature asks whether a business can extend its property interest in its physical servers to a quasi-property right, enabling it to exclude users from electronically accessing that server.[174] For example, a company might raise a cybertrespass claim to exclude unpermitted access that generates high load on the company's servers.[175]

Cyberproperty has not been broadly successful as a theory.[176] Ownership of physical hardware has nothing to do with the information that is stored on those servers.[177] The owners of the two interests are almost

173. *See* Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 88 (2003) (discussing "whether technological changes could ever lead us to abandon the presumption that a deliberate trespass counts as a private wrong," and arguing that this rule offers insufficient protection against "electronic snooping"); Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164–78 (2004) (exploring "how the law should treat legal claims by owners of Internet-connected computer systems to enjoin unwanted uses of their systems"); Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 23–43 (2007) (examining the history and development of cyberproperty); Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783 (2007) (focusing on the debate over property rules in the technology law context); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 470 (2006) (noting that there is an "overlap between contract claims and concepts of property"); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 521 (2003) ("Instead of concluding that cyberspace is outside of the physical world, courts are increasingly using the cyberspace as place metaphor to justify application of traditional laws governing real property to this new medium."); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 586–87 (2001) (analogizing website addresses and real property); Dan Hunter, *Cyberspace As Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 445 (2003) ("The application of the cyberspace as place metaphor within the criminal system is neatly reflected in the application, within the civil sphere, of the tort of 'trespass to chattels' in cyberspace.").

174. *See* sources cited *supra* note 173.

175. *See, e.g.*, Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003) (ruling on a claim of trespass filed by Intel against a former employee who sent mass emails using Intel's email system and determining that email communications that did not substantially impair the function of Intel's system did not constitute trespass to chattel).

176. *See* Lastowka, *supra* note 173, at 53 ("[L]ocating those property rights exclusively in the hands of chattel owners is not efficient.").

177. *See, e.g.*, Fairfield, *Virtual Property*, *supra* note 20, at 1052–57 (discussing types of virtual property, all of which have nothing to do with physical hardware); Edward Lee, *Warming Up to User-Generated Content*, 2008 U. ILL. L. REV. 1459, 1499 (2008) (explaining the proliferation of user-generated content).

never the same. Most servers are now virtual. Information is constantly in motion between server farms located in completely different parts of the world.[178] The servers are often maintained by third parties.[179] Digital resources are no longer tied to any particular physical asset from which a property interest might be bootstrapped.[180] The attempt to do so merely privileges those few companies that still maintain their own server farms.

The limits of cyberproperty theory demonstrate the need for well-conceived online property systems. There is every reason to believe that the degree of rivalrousness created by trustless public ledgers can restore the balance between intellectual and traditional property online. In a block chain, a slot in the ledger cannot be copied and cannot be duplicated. In solving the double-spending problem, trustless public ledgers offer a solution to the copying dilemma that has so hounded online property interests. The difficulty is that the technology has developed late, after a hybrid contract and intellectual property regime has become broadly accepted as governing even discrete and rival digital assets.

Done well, digital property could serve as a mainstay for consumer rights online.[181] Badly theorized digital property rules will not empower new owners in new spaces, but will merely act as a tool for extracting the benefits of the online environment for those with greater bargaining power.[182] Bad online property regimes increase information and other transaction costs and intensify unequal bargaining relationships. Compare, for example, the difference in bargaining power between Amazon and Kindle customers under the current anemic property regime for e-books with the relationship that would exist if customers held enforceable ownership rights in their book collections. Under the current regime, Amazon's power to revoke a person's entire online library in the event of a licensing dispute is merely a modernized version of the core unconscionability at issue in *Williams v. Walker-Thomas Furniture Co.*[183]

178. *See* R. Anthony Reese, *The First Sale Doctrine in the Era of Digital Networks*, 44 B.C. L. REV. 577, 635 (2003) ("Many copyright owners . . . will make regular backup copies of their works and store multiple backup copies in different locations.").

179. *See* Fairfield, *Virtual Property*, *supra* note 20, at 1081–82.

180. *See* sources cited *supra* note 177.

181. *See* Peter Lyman, *The Article 2B Debate and the Sociology of the Information Age*, 13 BERKELEY TECH. L.J. 1063, 1079 (1998) ("While the Article 2B debate focuses on the rights of the owners of digital property, it pays little attention to consumers' use of information, consumers' rights, and consumers' access to possible sources of economic power.").

182. *See* Bob Wright, *Technology and the Rule of Law in the Digital Age*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 705, 708 (2005) ("[T]he economic argument against digital theft . . . —as compelling as it is to business leaders—is remarkably ineffectual with the public.").

183. Williams v. Walker-Thomas Furniture Co., 250 F.2d 445, 448–49 (D.C. Cir. 1965).

What is obvious unconscionability when applied to personal property escapes notice when structured as an intellectual property license.

Additional theory is necessary to support a shift from the current hybrid contract and intellectual property regime to one that recognizes clean digital property interests.[184] The advent of block chain technology creates an opportunity to engage in this much-needed conceptual work. This part therefore offers a potential conceptual reboot for online property. It asserts that there is a serious need for robust online property interests that are neither tangible nor intellectual property. It offers a new view of property interests that may provide a more promising foundation for the future development of digital property law.

A. PROPERTY AS A LAW OF INFORMATION

Property has been variously conceptualized as the fruits of labor,[185] a means of anchoring personal identity,[186] or a way to maximize social

184. *See* Moringiello, *False Categories*, *supra* note 2, at 133 ("Despite the fact that the way persons communicate and do business has changed dramatically in the past fifteen years, we still lack an adequate vocabulary with which to describe intangible assets. With changes in business inevitably come changes in property rights and the business changes that developed with the growth of the Internet have similarly created a demand for new property rights.").

185. *See* Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L.J. 287, 301 (1988) ("[A]lthough one cannot physically possess or occupy ideas, property in ideas is justified because people 'have the right to enjoy the fruits of their labor, even when the labors are intellectual.'"); Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L.J. 1533, 1540 (1993) ("[O]ther courts have extended common law protection to intangibles on the Locke-like ground that no entity should 'reap where it has not sown.'"); Jeffrey S. Koehlinger, *Substantive Due Process Analysis and the Lockean Liberal Tradition: Rethinking the Modern Privacy Cases*, 65 IND. L.J. 723, 739 (1990) (discussing Locke's labor theory of value); Wendy J. Gordon, *An Inquiry into the Merits of Copyright: The Challenges of Consistency, Consent, and Encouragement Theory*, 41 STAN. L. REV. 1343, 1388–89 (1989) ("Many theorists, including John Locke, have attempted to justify dominion over property as an out-growth of rights over one's personal self, and an argument of that sort might also be used to justify intellectual property."); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1381–82 (2000) (discussing the distinction between a labor-desert theory of property and a utilitarian theory); Alfred C. Yen, *Restoring the Natural Law: Copyright as Labor and Possession*, 51 OHIO ST. L.J. 517, 517–22 (1990) ("If, as Locke intimated, labor were all that was necessary to give a person a natural right of property in an unowned object, then perhaps an individual's labor would be sufficient to make the ocean her private property."); William W. Fisher III, *Property and Contract on the Internet*, 73 CHI.-KENT L. REV. 1203, 1215 (1998) ("[P]roperty rights can and should be shaped so as to help foster the achievement of a just and attractive culture."); Diane Leenheer Zimmerman, *Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights*, 33 WM. & MARY L. REV. 665, 676 (1992) (explaining that Locke's theories had "a powerful effect in intellectual property and did much to legitimate the belief that ownership rights in speech originated deep in natural law and resounded with moral authority").

186. *See generally* Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957 (1982) (exploring the relationship between property and identity); Margaret Jane Radin, *Market-Inalienability*,

welfare through efficient allocation of resources in markets.[187] Each approach has had significant explanatory power for some property interests in some contexts. Yet no currently extant theory has provided an adequate foundation for bringing the virtues and values of property to the Internet.[188] Grant Gilmore stated the problem succinctly: "Even for a lawyer, the 'what is property?' problem presents no difficulty when you are dealing with goods, chattels, things: if you can see it, count, weigh and measure it, it exists; if you can't, it doesn't. But intangible claims are another matter entirely."[189] The consequences of the failure of property theory to

100 HARV. L. REV. 1849, 1852, 1903–36 (1987) (discussing market-inalienability based on a conception of personhood or "human flourishing"); Stewart E. Sterk, *Rhetoric and Reality in Copyright Law*, 94 MICH. L. REV. 1197, 1240–44 (1996) (discussing personal identity as a justification for broad copyright protection); Alice Haemmerli, *Whose Who? The Case for a Kantian Right of Publicity*, 49 DUKE L.J. 383, 488 (1999) ("As we have seen, . . . a Kantian right of publicity can be more expansively conceptualized as a property right grounded in human freedom . . . . It is true that enforcing publicity rights represents a value judgment that objectifications of personal identity constitute private property."); Kathleen M. Sullivan, *Unconstitutional Conditions*, 102 HARV. L. REV. 1413, 1485 (1989) ("Such a 'personhood' approach would hold that the opportunity to exchange rights for benefits wrongly commodifies rights. Especially when the government benefit comes in the form of money, but even when it is in kind, the condition attaches a price to the right surrendered—a value in exchange."); Diane Leenheer Zimmerman, *False Light Invasion of Privacy: The Light That Failed*, 64 N.Y.U. L. REV. 364 (1989) (discussing a personal right to privacy); C. Edwin Baker, *Property and Its Relation to Constitutionally Protected Liberty*, 134 U. PA. L. REV. 741, 747 (1986) ("The personhood function of property is to protect people's control of the unique objects and the specific spaces that are intertwined with their present and developing individual personality or group identity."); Justin Hughes, "*Recoding*" *Intellectual Property and Overlooked Audience Interests*, 77 TEX. L. REV. 923, 924 (1999) ("In the last few years, this generally pro-property personhood theory has been met with a scholarly reply specific to intellectual property: that owners' rights to control their intellectual property are really rights about who controls social meaning.").

187. *See* F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1, 44 (2004) ("An action then may be said to be conformable to the principle of utility . . . when the tendency it has to augment the happiness of the community is greater than any it has to diminish it" (quoting JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION 12–13 (J. H. Burns & H. L. A. Hart eds., Athlone Press 1970))); Michael A. Heller, *The Boundaries of Private Property*, 108 YALE L.J. 1163, 1222–23 (1999) ("[W]hen resources are wasted in a tragedy of the anticommons, protecting fragments of ownership does not serve the plausible economic goals of a private property regime."); Thomas W. Merrill & Henry E. Smith, *What Happened to Property in Law and Economics?*, 111 YALE L.J. 357 (2001) (discussing the "rise of the view among modern legal economists that property is simply a list of use rights in particular resources"); Neil Weinstock Netanel, *Copyright and a Democratic Civil Society*, 106 YALE L.J. 283, 347–48 (1996) (discussing copyright's importance to democratic civil society); Thomas W. Merrill & Henry E. Smith, *The Morality of Property*, 48 WM. & MARY L. REV. 1849, 1867 (2007) [hereinafter Merrill & Smith, *The Morality of Property*] (discussing morality and property rights); Henry Hansmann & Marina Santilli, *Authors' and Artists' Moral Rights: A Comparative Legal and Economic Analysis*, 26 J. LEGAL STUD. 95, 102, 142–43 (1997).

188. John Tehranian, *Parchment, Pixels, & Personhood: User Rights and the IP (Identity Politics) of IP (Intellectual Property)*, 82 U. COLO. L. REV. 1, 82–83 (2011).

189. Moringiello, *False Categories*, *supra* note 2, at 132 (quoting Grant Gilmore, *Article 9: What It Does Not Do for the Future*, 26 LA. L. REV. 300, 301 (1966)).

adequately account for rival and intangible property interests have been significant: an online ecosystem in which consumers control little and own even less.

This section proposes to bridge the physicality divide in property law by asserting that property rights are best understood as information and that property systems are ones in which the form of the property as well as the means of its transfer are methods of conveying information. This section as a whole argues that property is not the law of things (at least insofar as thing-ness implies tangibility), but is instead a law of information that conforms to identifiable rules of information management and flow.

Although current theory does not conceive of property as pure information, there has been much important thinking on the information costs of different property forms and rules. Property is, under the view of the information cost literature, an emergent product of the informational characteristics of property forms. Specifically, property forms are a function of the information that such forms convey to owners and third parties. Through these forms, owners know what they can do with resources, and third parties know what they cannot do. Communicating which parties may do what with which resources at the lowest cost is property's project.

The following subparts therefore first consider information cost theory before discussing a potentially useful addition to that theory. Where prior theory has analyzed property in terms of information costs, this Article takes the next natural step and treats property itself as an information system.

1. Property and Information Cost Theory

Henry Smith and Tom Merrill have spearheaded renewed interest in examining the information characteristics of property forms. Smith and (to some extent) Merrill object to the "bundle of sticks" view of property on the grounds that removal of a stick from the bundle disrupts the fundamental informational clarity of the thing.[190] In their terminology, if I buy a bicycle for which I have all the sticks except the right to ride it on Tuesdays, the fundamental integrity of the bicycle as a thing that one may buy, sell, use, and exclude others from using is damaged.[191] Others will

190. Merrill & Smith, *The Morality of Property*, *supra* note 187, at 1851.

191. Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The* Numerus Clausus *Principle*, 110 YALE L.J. 1, 26–28 (2000) [hereinafter Merrill & Smith, *Numerus Clausus*] (illustrating how creating property rights imposes "measurement costs . . . on strangers to the title").

have to engage in expensive investigation to determine whether the bicycle they are about to buy can be ridden on Tuesday or whether that right has been quietly sold.[192] Thus, the removal of the property "stick" compromises the informational integrity of the object.[193]

Instead, Merrill and Smith proposed that property can best be explained as the process of optimizing property rights by reducing information costs for search, verification, or transfer. The literature can be divided into two parts. First, Merrill and Smith addressed the range of property forms. This is termed the *numerus clausus*: the notion that the range of property forms should be a predetermined and closed set.[194] Second, as Smith has recently written, individual packages of property rights move more smoothly in the stream of commerce when they are cleanly delineated and modular, so that each module can, like legal legos, be transferred or rearranged into new and useful forms with minimum transaction costs.[195] This subpart addresses each in turn.

The *numerus clausus*, meaning "the number is closed," is a principle limiting the number of property forms.[196] Parties are not free to vary the form of property by contract. If parties attempt to create a new property form, the rights are recognized as contractual but do not bind third parties

192. *See id.*

193. *See id.*

194. *Id.* at 4.

195. *See* Henry E. Smith, *Modularity in Contracts: Boilerplate and Information Flow*, 104 MICH. L. REV. 1175, 1187 (2006) [hereinafter Smith, *Modularity in Contracts*] (clarifying the role of modularity in reducing transaction costs).

196. Johnson v. Whiton, 34 N.E. 542, 542 (Mass. 1893) ("A man cannot create a new kind of inheritance."); Bernard Rudden, *Economic Theory v. Property Law: The* Numerus Clausus *Problem*, *in* OXFORD ESSAYS IN JURISPRUDENCE: THIRD SERIES 239, 243–44 (John Eekelaar & John Bell eds., 1987); Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 4, 13 ("[C]ourts enforce the *numerus clausus* principle strictly (although not of course by name) in the context of estates in land."); Richard A. Epstein, *Liberty Versus Property? Cracks in the Foundations of Copyright Law*, 42 SAN DIEGO L. REV. 1 (2005); Abraham Bell & Gideon Parchomovsky, *Property Lost in Translation*, 80 U. CHI. L. REV. 515, 541 (2013); Thomas W. Merrill & Henry E. Smith, *The Property/Contract Interface*, 101 COLUM. L. REV. 773, 790 (2001) [hereinafter Merrill & Smith, *Property/Contract*]; Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The* Numerus Clausus *Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. 373, 374 (2002) (arguing that the *numerus clausus* doctrine aids verification of ownership rather than serving to standardize property forms); Henry E. Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 YALE L.J. 1742, 1780 (2007); Henry E. Smith, *The Language of Property: Form, Context, and Audience*, 55 STAN. L. REV. 1105, 1160 (2003) [hereinafter Smith, *The Language of Property*]; Fairfield, *supra* note 20, at 1051–52; Hanoch Dagan, *The Craft of Property*, 91 CALIF. L. REV. 1517, 1565–70 (2003); Heller, *supra* note 187, at 1176; Michael A. Heller, *The Tragedy of the Anti Commons: Property in Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998); Daphna Lewinsohn-Zamir, *The Objectivity of Well-Being and the Objectives of Property Law*, 78 N.Y.U. L. REV. 1669, 1730 (2003); J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 802–03, 810–13 (1996).

as would a property interest.[197]

Merrill and Smith's answer as to why property law should be so constrained, at significant cost to the satisfaction of individualized preferences, is that the limitation of form creates information cost savings.[198] Constrained choice means lower search and verification costs. If the savings generated by a reduction in information costs are greater than the efficiency loss engendered by constraining choice, the limitation on forms increases social welfare.[199] Consider buying batteries. If there were only one kind of battery, then purchasing a battery would be simple. The more kinds of batteries there are, the more effort one must invest in determining the correct battery to purchase.

Choice raises information costs. It also increases satisfaction. The question is how to best balance the range of choice that increases individual satisfaction with the information costs increased by that range. This is an optimization exercise.[200] Increased choice beyond a certain point (see: cable channels in the United States) does not increase human happiness. Overly constrained choice (see: television channels in Germany) decreases the degree of fit between human desire and result, which decreases utility.

The *numerus clausus* as envisioned by Merrill and Smith is a principle of data management. It sets requirements for data format through its restrictions on property forms.[201] Consider property as a check-box menu.[202] One must select the property type: leasehold (subcategories: term of years, periodic tenancy, tenancy at will, and tenancy at sufferance),[203] freehold (subcategories: fee simple absolute, determinable, subject to condition subsequent, subject to executory limitation), life estate, future interest, or limited right (subcategories: easements, covenants, servitudes, profits). Those transactions in which the proper datafields are correctly entered pass with minimum friction through the system and are enforced by courts. Those which do not are not enforced against third parties, although

197. Hansmann & Kraakman, *supra* note 196, at 378.

198. Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 26.

199. *See id.* ("In the potential transfer situation, the individual will measure as long as the marginal benefit in reduced error costs exceeds the marginal costs of measurement.").

200. *See id.* at 69.

201. *Id.* at 33; Moringiello, *Virtual Worlds*, *supra* note 28, at 188–89.

202. *See* Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 7 ("When unsophisticated or poorly advised actors enter these worlds, they may find that courts force the transaction into one of the established 'boxes,' with the result that the actors' intentions are frustrated."); *id.* at 12 ("The common-law system of estates in land is an area of property law universally recognized to have a 'formalistic, box-like structure.'").

203. Merrill & Smith, *Property/Contract*, *supra* note 191, at 832; Moringiello, *Virtual Worlds*, *supra* note 28, at 185.

they may be enforced contractually.

Merrill and Smith's view that increased range of property formats increases data costs to third parties has not gone untested. In offering a critique of Merrill and Smith, Hansmann and Kraakman ask why the addition of marginal novel property forms would necessarily impact pre-existing forms.[204] For example, the fee simple absolute might not become more confusing as a property form just because a new and different form was added to the list of forms. One answer to this criticism is that new forms dilute the informational clarity of existing forms because a non-transacting party does not know which form she is receiving *ex ante* and must investigate.[205] This answer is, however, slightly too simple. Beyond a certain basic number of forms, the addition of marginal forms is unlikely to increase information costs as much or even at all. A more developed version of the criticism would be, therefore, that the addition of each marginal additional form of property does not linearly increase information costs.[206] As soon as there are two property forms, the need to verify the form of the property obtains. Once someone must check to verify the form of the property anyway, additional, marginal possibilities for that form raise transaction costs much less. The information cost difference between one and two forms of property is significant. The information cost difference between the thousandth and the thousand-and-first form of property is not.

2. Property, Information, and Modularity

The second major line of thought in considering the information characteristics of property is the question of modularity, or how cleanly the information of a property form is packaged, and how smoothly each piece of property or property right interfaces with each other piece or right. The modularity discussion is highly salient to the project advanced here: developing a system for securely transferring property interests in the form of packets of information. For digital property to attract users, it must offer discrete, well-defined, constrained, and simple sets of rights.

Information costs can be reduced not only by limiting the range of property forms, per the *numerus clausus*, but also by optimizing the data characteristics of a particular property form by making it modular. The

204. Hansmann & Kraakman, *supra* note 196, at 380–81.

205. *See* Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 33 ("Limiting the number of basic property forms allows a market participant . . . to limit his or her inquiry to whether the interest does or does not have the features of the forms on the menu.").

206. *Id.* at 39–40 & fig.2.

numerus clausus discussion, above, focused on eliminating additional property forms that impose search and verification costs on owners, potential third parties, creditors, and others. The modularity discussion is conceptually distinct.[207] The focus is not on novel property forms that expand the range of options through which third parties must search, but on the packaging of information about property such that there are constrained and clear information inputs and outputs.[208]

Modularity is a function of what Smith calls "nearly decomposable" systems.[209] That is, modules encapsulate complexity, and interface points between modules are chosen for their simplicity. Modularity creates simplicity by breaking problems up, encapsulating repeated and complex interactions together, and then creating a neat and clean interface for the rest of the system.

Modularity is both a method of information transfer and an information cost reduction strategy. Someone seeking to use the system need only deal with, change, or modify one module at a time. Consider the common practice of cleaning a messy room by putting toys away in a box. The same chaos reigns inside the box that previously affected the entire room. Yet the packaging of the box has made the mess modular.[210] The box fits on a spot on the shelf. If a child seeks a specific toy and the boxes are properly labeled, she need only search through the single box rather than destroy the room searching through all the toys. Once the single toy is found, the box can go back on the shelf, and the room is again clean.[211]

Or, consider the modular design of a car. Those parts that are sufficiently tightly connected to one another are fitted together into a unit. Complexity is contained with the unit, and outputs and inputs of the unit are simplified. A given part that fails (usually my water pump) can be removed and replaced without disrupting the entire system, since any unit that performs that function and matches the inputs and outputs can be

207. *See* Smith, *Modularity in Contracts*, *supra* note 195, at 1176 ("[M]odularity is a device to deal with complexity by decomposing a complex system into pieces (modules), in which communications . . . are intense within the module but sparse and standardized across modules."); Joshua A.T. Fairfield, *The Cost of Consent: Optimal Standardization in the Law of Contract*, 58 EMORY L.J. 1403 (2009) (discussing standardization and innovation through the concept of modularity).

208. *See* Smith, *Modularity in Contracts*, *supra* note 195, at 1180 ("Forming a modular system involves partially closing off some parts of the system and allowing these encapsulated components to interconnect only in certain ways.").

209. *Id.* at 1196.

210. *See id.* at 1176.

211. *See id.* at 1180 ("[A]djustment can happen within modules without causing major ripple effects.").

exchanged for any other. Or, for those who build their own computers, consider the modularity of RAM sticks. Enormous numbers of tiny parts are layered together and given one clean interface with the rest of the system. The complexity of the RAM stick is contained and packaged neatly, so that a user need only slot the stick into the computer.

Modularity, like the *numerus clausus*, helps to explain property characteristics and forms in terms of information costs. To this point, the literature of information cost theory has done critical work setting the stage for a theory of property as information. But current theory does not sufficiently theorize property itself as information. Even the information cost view of property remains strongly tied to physical objects. Remaining bound to the physicality and tangibility of property poses a barrier to the effective use of information cost theory to ground a robust and working system of online property, as the next subpart explores.

3. Property Is a Law of Information, Not Things

If one accepts that information theory is central to the understanding of property, the next step is to understand that property is itself an information system. Extant theory on information costs in property pulls up short, recognizing the importance of information to property forms without recognizing that property forms are themselves information. Instead, the information cost literature doubles down on the concept of property as the law of things. For example, Smith writes: "I argue that the baselines that property furnishes, as well as their refinements and equitable safety valves, are shaped by information costs. For information cost reasons, property is, after all, a law of things."[212] Thus, "[a]n 'in rem' right originally meant a right 'in a thing,' and [Smith argues] that it is the mediation of a thing that helps give property its in rem character—availing against persons generally."[213] In this sense, the law gives a "special respect . . . to physical objects [because] the objects themselves provide an excellent form of fixed rule. The contours of an object . . . establish a boundary that is highly resistant to revision in a particular dispute."[214]

Treating property as the law of things, at least without a more nuanced

212. Henry E. Smith, *Property as the Law of Things*, 125 HARV. L. REV. 1691, 1691 (2012) [hereinafter Smith, *Property as the Law of Things*].

213. *Id.*

214. Henry E. Smith, *Property and Property Rules*, 79 N.Y.U. L. REV. 1719, 1765 (2004) [hereinafter Smith, *Property Rules*] (quoting Emily Sherwin, *Two and Three-Dimensional Property Rights*, 29 ARIZ. ST. L.J. 1075, 1091 (1997)). *See also* Louis Kaplow & Steven Shavell, *Property Rules Versus Liability Rules: An Economic Analysis*, 109 HARV. L. REV. 713, 721 (1996) (noting the strong preference for property rule protection of physical things).

idea of the informational role of thing-ness in property law, would be a lost opportunity. The risk is that any enhanced understanding of the informational role of property would be limited to tangible things. The old trouble would return: property law would continue to inadequately address intangible property rights that do not fit squarely within intellectual property law and would leave traditional property theory with no conceptual approach that fits naturally in online environments. The next subpart therefore engages the argument that property is the law of things. It proposes a friendly amendment to the extant literature. Properly understood, "thing-ness" in property law need not exclude online or digital objects. (Indeed, Smith suggests such a tack in passing.)[215] Things are just one subset of information objects. To see this clearly, it is useful to distinguish between a thing and an information object, discussed below.

a. Thing-ness in Property Law

For Smith, thing-ness is essential to modularity.[216] Ownership rights in a thing may be complex, but that complexity need not reach third parties. Consider Blackacre.[217] Property rights between owners may be complex—interest holders may be remaindermen, joint tenants, renters, or any one of a range of other possibilities, yet all the potential third party trespasser need know is to keep out. As Merrill comments on Smith:

> The proverbial Blackacre presents a simple rule of exclusion insofar as the audience of strangers is concerned, a complex of formal rules when potential transactors enter the picture, and a potentially limitless diversity of rules and norms when the relevant audience consists of insiders such as co-owners.[218]

Essential to Smith's conception is the idea of a thing. Blackacre as a thing carries informational content. The land in this example serves as a proxy for the significant complexity going on inside the property form. A potential trespasser need not become embroiled in the machinations of interest holders in the property; she need only know that to enter another's land without permission is trespass.

215. *See* Smith, *Property Rules*, *supra* note 214, at 1754 ("The intuition that property rules are particularly suited to the protection of things—and, unlike some, I include here intangible things—is no accident."). *See also* Smith, *Property as the Law of Things*, *supra* note 212, at 1703 ("Property clusters complementary attributes—land's soil nutrients, moisture, building support, or parts of everyday objects like chairs—into the parcels of real estate or tangible and intangible objects of personal property.").

216. Smith, *Property as the Law of Things*, *supra* note 212, at 1700–08.

217. *See* Thomas Merrill, *Property as Modularity*, 125 HARV. L. REV. 151, 151 (2012).

218. *Id.*

Yet here the argument for thing-ness, at least in the purely physical sense, fails. The metes and bounds of Blackacre are not necessarily physical, they are informational. Blackacre does not, properly understood, exist apart from the information that defines its existence. The rocks, trees, and land exist, of course, but they are not Blackacre. Blackacre is comprised of information delineating and demarcating the land. There is usually no physical line that demarcates the property from neighboring land. Thing-ness is simply information about the limit of rights. This is true even when there is an objectively discernable physical boundary to property. To take an example from chattel property: if I own a small framed picture, I might own 1' x 2' of painted canvas. If I own a larger picture, I may own 2' x 3'of painted canvas. The limit of the frame and the concept that the picture is a unified "thing" (even though it is a composite of paint, medium, backing, frame, and wire) serve to limit information costs and make the picture modular, easily transferrable, sellable, and so forth.

An overemphasis on physical rather than informational thing-ness interferes with the information theory of modularity. Modules manage complexity by packaging interrelated parts together.[219] Those parts are often themselves modules. Thus, a car is a module, but the parts of which it is made are also modules. Smith notes this expressly as one of the strengths of modularity in property: that property modularity allows the creation of nested structures through limited recursion.[220] But it also means that "thing-ness" is itself something of a false construct. The thing-ness of a car is decomposable to the thing-ness of its parts, which are in turn decomposable to the thing-ness of components, which are of course themselves further decomposable. "Thing-ness," in the tangible sense, does not tell us which thing, the component, the part, or the car, is the fundamental unit of property. To mistake thing-ness, especially familiar physical thing-ness, for the *sine qua non* of property, instead of the information properties thing-ness represents, would sap much of the strength of information cost theory as applied to property.

Rather, the same techniques of managing information costs by constraining search costs and managing complexity by providing interface points of constrained information inputs and outputs are the bedrock of coded environments. These principles are not about thing-ness at all. Instead, thing-ness is one way among many to manage information flow by

219. Smith, *Property as the Law of Things*, *supra* note 212, at 1701.
220. *Id.* at 1707–08.

creating simple interfaces between data modules. It should be possible to usefully amend information theory in property so as to preserve its value in creating digital property systems. The following subpart therefore addresses how information systems manage informational complexity through modularity, before drawing some insights from information system design for property rules.

b. Object Oriented Programming

Property is not the law of things, it is the law of data objects, whether those objects are transferred by physical exchange or by changing a ledger entry in a database.[221] One way to see this is by analogy to computer code. Code is a chain of logic, in which one action is logically defined along a specific path, to lead to another action. Code can be written with long, untrimmed chains of input and output variables, in which each action is tied to numerous other actions. This tangle of logic is often referred to as "spaghetti logic." Such code does not manage complexity by limiting and simplifying the interface points between different parts of the code.

Better-designed code creates "objects" that act, in an informational sense, like Smith's "things," although they have no tangible or physical component. An object in code is a package of functions that produces a simplified output useable by the rest of the system. For example, imagine a system designed by a bank to determine whether to make a loan to a customer. One might design code that ties each input to each output—the effect of the economy on the client's future income, for example. The result might be very accurate but also complex and difficult to change. A different way of organizing the code would be to write one module, or object, that would package all of the relevant factors together and spit out one number: the interest rate at which it is currently profitable for the bank to extend loans. Any number of considerations might go into such a determination, yet the module spits out a single number. That number, then, is the interface with other modules in the system. Those modules need not recreate the entire sequence of logical manipulations that the interest rate module did, they merely need to call the output variable of the interest rate module. In the same way, the customer's ability to pay might be a function of a range of different variables reduced to a single number. That number, too, can be passed to the rest of the system. The value in separating these

221. *See* Margaret Jane Radin, *Boilerplate Today: The Rise of Modularity and the Waning of Consent*, *in* BOILERPLATE: THE FOUNDATION OF MARKET CONTRACTS 189, 189 (Omri Ben-Shahar ed., 2007) ("Modularity became important to physical architecture in the first part of the twentieth century and to the virtual architecture of computer science in the later twentieth century.").

modules out is that if one needs to change a component, one can do so without disrupting many ties throughout the system. By intentionally bottlenecking information flow between modules, a coder can ensure that a change in one internal function does not disrupt the entire system. One need not chase down every end of every tangled piece of logical spaghetti.

Modularity is, in a way, inefficient. It may be that a direct connection between general economic bellwethers and income might produce a more accurate estimate of income. Coders might be tempted to kludge connections between every relevant input and the output they seek. But in doing so, they lose the organizational structure of the code that makes it easy to understand, maintain, pass on, swap out, and most of all reuse in other coding environments. Once a good code object has been created, it can be swapped out like a Lego piece to build entirely different structures.

c. Object Oriented Property

"Things" in property, like objects in code, are packages of closely related data functions. Property systems and forms do not directly convey physical assets, they convey packages of information. Property law does not simplify things (at least not directly), it simplifies information flows. Thus, property is the law of data objects, not the law of physical things. Physicality of course creates certain data characteristics (uniqueness, rivalrousness, persistence, and the delineation of a package of rights as tied to the delineation of the "thing") as natural byproducts, but we do not need physicality to create clean data objects. Coders do not rely on tangible thing-ness at all when they create modules that constrain information flow to make the code more manageable. In the same way, digital objects do not need physical thing-ness to benefit from the virtues of a property system.

Constraining and modularizing property forms ensures that the information at the core of property is packaged in a way that can be moved smoothly through the stream of commerce. But it is possible to mistake these features for the point. For example, Merrill expresses concerns about the modularity approach to property because it "fails to explain the limited number of legal forms in which property can be held—the *numerus clausus* principle."[222] It certainly does not, but this does not matter. Modularity does not cause or explain the *numerus clausus*. Both the *numerus clausus* and modularity proceed from the same principle: property is information.

Indeed, both the *numerus clausus* and modularity cease to be property principles when they conflict with principles of efficient information flow.

222. Merrill, *supra* note 217, at 154.

For example, Smith discusses recursion: the ability to reuse modules in a nested form to create new property structures (such as parts in a car, noted above).[223] However, recursion does not always reduce information costs. Recursion can increase complexity when it is unlimited. Consider, as an example of unbounded recursion, the famous wish for more wishes. While the ability to do again what a system has done before is a core function of automation, recursion is not an unlimited positive in information theory. It is famously simple to trap information systems in an infinite loop with recursion. Although the trope of Captain Kirk confusing a computer adversary by posing a logical loop is campy,[224] it conveys an underlying truth: long or infinite recursive loops can damage and delay information systems. The same is true for property systems. Recursive forms like the fee tail have been abandoned, and rules against dead-hand control, such as the rule against perpetuities, limit the grantor's ability to recursively "reset" ownership of land. Property systems, like other information systems, protect themselves by limiting the number of times a recursive loop can run on the system.

Property shares the considerations of object oriented programming and many of its tools for managing information flow. The guiding principle is one of information management: of rapid, effective, secure, and verifiable information flow based on property forms. The next section therefore bears down on this element of property: that property law forms a protocol for the transmission, security, and verification of information, at reduced cost. Or, more simply, if property is information, property systems are information protocols.

B. THE PROPERTY PROTOCOL

The value of information cost analysis of property extends well beyond property forms, to the system for conveying and verifying property information. This section therefore outlines some principles of information design that might further enable property systems to do the job of conveying the core information of property at lower cost with increased certainty.

If property is information, property systems are a protocol for communicating, verifying, and protecting that information. To transfer land from one person to another, one must transfer the information (the deed)

223. Smith, *Property as the Law of Things*, *supra* note 212, at 1701.

224. *See Star Trek: The Original Series: The Changeling* (NBC television broadcast Sept. 29, 1967).

that identifies the transaction (sale or ownership) and ties the successor identity (buyer) to the resource (the land). To buy an MP3, one must record the information (on a watermark or license server) that identifies the transaction (license) and ties the successor identity (the consumer) to the resource (the music). To generate a security interest, one must record the information (in a UCC filing) that identifies the transaction (security interest) and ties the secured party (usually the bank) to the resource (the debtor's collateral).

The traditional definition of property as the relationship of actors to assets and to each other does not fall far from the mark.[225] But the traditional definition does not capture the degree to which property systems not only require, but are in fact comprised of, information. The key player in a property transaction is not the seller or the buyer, but the non-involved third party, who is bound by the dispositions made by the negotiating parties.[226] The directly involved parties of course already have information about the deal through their contract negotiations. They need no property system to apprise them of the terms of their own deal. That can be handled through contract rules designed to foster bilateral information disclosure.

By contrast, a true property system must deliver information to third parties.[227] First, non-parties need information about transactions with which they are not at all involved. Assume A and B transact in land. Party C needs to know the boundaries of the transaction entered into by A and B, which constrains where C may hunt or fish.[228] Further, non-parties need information about transactions with which they are not involved *yet*. Assume C wishes to buy the land from B. She will need information about the A-B deal and all earlier deals.[229] Finally, C needs access to change the information, that is, the records, should she decide to become owner of the land.[230] The common thread is information. The essence of the property system itself is not the identity, asset, or relationship between the parties, it is the information about those elements, and the degree to which that

225. *See* Moringiello, *False Categories*, *supra* note 2, at 134 (noting the "widely accepted definition of 'property' as the 'relations among people with regards to things'" (quoting JOSEPH WILLIAM SINGER, INTRODUCTION TO PROPERTY § 1.1.1 (2d ed. 2005))).

226. *See* Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 33 (discussing how "to control the external costs of measurement to third parties").

227. *See* Michael Trebilcock (Corresponding Author) & Paul-Erik Veel, *Property Rights and Development: The Contingent Case for Formalization*, 30 U. PA. J. INT'L L. 397, 411 (2008) ("[A] formal property system can also reduce transaction costs in market interactions by providing increased information to third parties about the rights that an individual has over land.").

228. *See* Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 33.

229. *Id.*

230. *Id.*

information is effectively stored, communicated, and verified.

Procedures for quickly, effectively, securely and cheaply communicating information are, in information parlance, called protocols.[231] A protocol sets the format for data.[232] It sets the procedures for transmitting it. It determines to whom certain data should be sent. It sets the procedures for error checking and the procedures for confirming that the data has been received. It determines the routing procedures for moving the data through a network. It sets procedures for lost or missing data.

I propose that a property system is an information communication and storage protocol. There are good protocols—ones that permit maximum information flow, accuracy, and security, and cause minimum confusion and resistance. There are bad protocols—ones that engender confusion, noise, uncertainty, and insecurity. Similarly, there are good property systems—ones that permit transactions at high velocity, with high security, and with low friction. There are bad property systems—ones that are time consuming, costly, insecure, and inaccurate. The virtues are the same, and so are the vices. Good property systems transmit information about who may do what with which resources rapidly and securely, secure it faithfully, and can verifiably reproduce it. Bad property systems fail at each of these tasks.

Conceptualizing property systems as information protocols has distinct advantages over extant property theories. As worked out above, physical things themselves are not the heart of property.[233] The bundle of sticks—whether an owner may use, exclude, alienate, or destroy—is not the heart of property. Personal identity is not the heart of property. Instead, a theory of property as the data consisting of *who* may take *which action* with respect to *what asset*, and the procedures for communicating,

231. *See* Brett M. Frischmann & Mark A. Lemley, *Spillovers*, 107 COLUM. L. REV. 257, 294 (2007) ("The current Internet infrastructure evolved with the so-called 'end-to-end' design principle as its central tenet. This design principle is implemented in the logical infrastructure of the Internet through the adoption of standardized communication protocols (e.g., the Internet Protocol suite)."); Julian Chokkattu, *Bridging The Gap As The Smart Home Industry Expands*, TECHCRUNCH (July 7, 2014), http://techcrunch.com/2014/07/07/bridging-the-gap-as-the-smart-home-industry-expands/ ("[T]ech giants Google and Apple are just a few companies that have been looking to bridge connectivity to different branded products with wireless communications protocols and break this fragmentation.").

232. Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 91 (2003).

233. *See* Moringiello, *False Categories*, *supra* note 2, at 134 ("As Gilmore noted forty years ago, . . . in asking property questions, we commonly conflate rights in things with the things themselves.").

changing, verifying, and storing that data, cuts closest to the bone. As one transaction follows another, forming a chain of title, we create a chain of data relating each transaction to the next. The property system resides in the procedures for tracking, transmitting, and verifying that information. A property system enables transfers by conveying the information about who now owns what. A property system enables exclusion—the most commonly discussed element of property systems—by relating a *what* to a *not-who*, that is, the set of people who are barred from making use of a resource.

The received wisdom that traditional property is somehow foreign or alien to information environments is incorrect. This error stems from the underexplored and incorrect assumption that property is about physical things, or about identity, or about specific actions one may take with property. Identity, assets, and actions are all important parts of a functioning property system, but they are not its substance. The substance of property is information. If property systems are information systems, then it must be possible to implement them in an information environment.

To test whether property-as-information-protocol can hold conceptual water, it is useful to consider a few of the virtues of good information communication and storage protocols, and to observe whether they have explanatory power in the property context. Although there are many descriptors of good communications protocols, three are discussed here, loosely grouped around data at rest before it is sent, data in transit, and data at rest after it has been received. The following subparts first describe how these characteristics work in information environments before drawing parallels to characteristics of property systems.

1. Data Formatting

A major challenge to information systems is ensuring that data follows a simple format such that it can be transferred or searched with minimum cost. Information can come in an infinite range of forms, some sufficiently organized as to be useful to automated systems, and some so disorganized as to be useless to anyone. Good data formats include necessary data and exclude data—even relevant data—when it appears in a format that makes parsing, processing, storage, or later accurate retrieval of the data more difficult. A good data format constrains information to the essential fields necessary for the transfer, storage, and retrieval of that information. Further, the format constrains the range of ways in which information can be entered. It selects a standard.[234] Such standards necessarily exclude useful but more costly means of presenting information in favor of an agreed-upon form.

The law of property operates as an information protocol in that it sets standard formats for data. Assume that there is only one property format: FSA (fee simple absolute). Under this regime, there are serious utility costs due to constrained ability to satisfy preferences, but there are no information costs. The recipient need not inquire as to the form of property she receives. Now, assume we add a new hypothetical format: FSB. A recipient must now inquire as to whether she is receiving FSA or FSB, and costs rise. Here, we see Merrill and Smith's information cost model at work.[235] But to incorporate Hansmann and Kraakman's criticism,[236] assume that we add an additional marginal format: FSC. The costs for verifying the format of the property do not change. All that one must do is exclude all results that are not FSA. To think of it another way, if one desires FSA, one need not bother with all other formats, FSB through FSZ. One must check, but as long as labels are clear, it is just as easy to see that FSH returns a result of "no, this isn't what I want," as it is to see that FSQ returns a result of "no, still not what I want."

Theorizing the *numerus clausus* as a data format rule provides a friendly amendment to Merrill and Smith's theory, and addresses the critique that, as property forms are added, the marginal additional transaction cost steeply declines. The problem is not the total number of forms, but the ability to differentiate between forms. Property forms must be more than merely a little different; they must be different enough so as to be distinguishable. The *numerus clausus* as amended here is therefore a principle of the minimum difference necessary for differentiation. What is necessary—and indeed, what property law offers at its core—is a system of specific, constrained, parameterized property forms that are detectably different from one another at low cost. The dangerous case is one in which a given property format (say, FSA2) becomes confused with another (say, FSA), such that one can check and still not know what format the property takes. Worse is one in which a non-standard property form looks the same as a mainstream, common property form on the surface, but is actually different due to obscure or hard-to-obtain information.

234. The term "standard" is used here and throughout this Article in the technical sense of an agreed-upon format for the transaction, and not in the legal sense of a fuzzy legal line.

235. Merrill & Smith, *Numerus Clausus*, *supra* note 191, at 27.

236. *See* Hansmann & Kraakman, *supra* note 196, at 380–81 (arguing that the addition of property forms would not necessarily generate a "meaningful degree of confusion").

A theory of property as information resolves much apparent contradiction. With Merrill and Smith, I treat information costs as central to the law of property. With Hansmann and Kraakman, I note that marginal property formats do not linearly increase information costs.[237] Finally, I build on extant theory by noting that it is the ability to distinguish between formats—and not the raw number of forms—that matters in creating a low cost and high velocity property system.

2. Verification and Error Checking

Verification is a vital component of information protocols, and by extension property systems.[238] The value of information lies not merely in its content, but also in the degree of certainty that the information was not altered or corrupted in transit. Verification matters most if information is to be passed further along to another party or another information system, further spreading corrupted data. The flip-side of verification rules are error-clearing rules. These rules exclude corrupt data so that it does not get passed forward. Some error in a one-time transaction does not matter much. Matters are different for information that must be passed forward based on the prior chain of events. Accumulation of errors within a data chain, just like the accumulation of clouds on title in a chain of title, will eventually crash an information system or render an asset immobile in the stream of commerce because title is too clouded.

Property systems have extensive error checking rules. For example, title searches serve as a form of error checking for title-based systems. The purpose of the search is not merely to make sure that the asset is sufficiently unencumbered such that the buyer is not buying a lawsuit along with her asset, but also to ensure that the information stream attached to the asset is itself not so clouded or contaminated that the buyer would have trouble selling the property forward.[239] Similarly, when courts pay attention to flaws in chains of title, they encourage prospective buyers to focus attention on the chain of data. Many problems that are fixed as a result of

237. *See generally id.* (discussing verification rules in property).

238. *Id.* at 374, 380.

239. *See*, *e.g.*, Feit v. Donahue, 826 P.2d 407, 409 (Colo. App. 1992) ("[The] grantee under a warranty deed, except for matters specifically enumerated therein, should be in much the same position as [a purchaser of land with the] right to demand title which will put him in all reasonable security against loss or annoyance by litigation and will enable him not only to hold his land but to hold it in peace." (alteration in original) (quoting Fechtner v. Lake Cnty. Savs. & Loan Ass'n, 361 N.E.2d 575, 578 (Ill. 1977))); Chavis v. Gibbs, 94 S.E.2d 195, 197 (Va. 1956) ("The main purpose of recordation statutes is to give constructive notice to purchasers and encumbrancers who acquire or seek to acquire some interest or right in property.").

title searches are minor errors in the data chain, and clearing up small errors prevents aggregation and improves the overall health of the registry.

Error clearing rules also abound in the law of property. For example, rules of many different stripes protecting the rights of bona fide purchasers and buyers in the ordinary course of business clear accumulated clouds on title.[240] These rules operate to insulate current transactions from errors in prior transactions. For example, buyer in the ordinary course of business rules ensure that when one purchases a flat screen television from Best Buy, one need not be concerned with whether Best Buy has granted Bank of America a security interest in inventory.[241] If a consumer sells the flat screen to another consumer, a different flavor of the same rule applies to clear other complicating security interests that the seller might have left still attached to the property.[242] Sales law's rules for voidable title and entrustment ensure that bona fide purchasers for value and buyers in the ordinary course are insulated from upstream title conflicts by clearing title error in the hands of the purchaser.[243] Or consider marketable title acts for real estate, which only require a search back up the chain of title for a statutory period of years.[244] All prior transfers are considered good and do not interfere with the registered chain of title. These rules for both real and personal property have as many different variants as contexts, but each has the salutary function of clearing errors in the chain of title so that mistakes in prior transactions do not aggregate to immobilize the asset.

3. Data Security

The third major category is data security.[245] Data must be secure both in transit and at rest. Data must be routed to the proper recipient and not to a third party who fraudulently attempts to stand in the shoes of the sender

240. *See, e.g.*, Sender v. Cygan (*In re* Rivera), 513 B.R. 742, 753 (Bankr. D. Colo. 2014) ("Colorado is a race-notice state where no unrecorded instrument is valid against a *bona fide* purchaser of the subject property who first records. Consequently, as long as an instrument is properly recorded, subsequent purchasers have an obligation to find it at the county clerk and recorder's office and are considered to have constructive notice even if they do not locate it."); U.C.C. § 9-320(a) (2010) ("[A] buyer in ordinary course of business . . . takes free of a security interest created by the buyer's seller, even if the security interest is perfected and the buyer knows of its existence."); *id.* § 2-403(1) ("A person with voidable title has power to transfer a good title to a good faith purchaser for value.").

241. *Id.* § 9-320(a).

242. *Id.* § 9-320(b).

243. *Id.* § 2-403.

244. *See, e.g.*, Unif. Marketable Title Act § 3(a) (1990) ("A person who has an unbroken record chain of title to real estate for 30 years or more has a marketable record title to the real estate . . . .").

245. There are, of course, other virtues of information protocols, which are excluded here due to space constraints. Routing and addressing are major goals of a good transfer protocol. The data must go to the party to whom it is addressed.

or receiver. The question is whether these values are a core part of the law of property.

Security has always been a feature of property. Gold has always been kept in vaults. But the argument that security is a core and integral part of property law is less immediately intuitive than it is for data formatting, error checking, and error clearing. The security surrounding an asset has rarely been directly conceptualized as a key element of the property itself. Lack of built-in security has long been a driving factor for property law. Developed rules preventing theft, trespass, and conversion are necessary because property, especially personal property, is so easy to steal, subvert, or convert.[246]

The strongest difference between property rules and information security principles is that most property rules secure property by *ex post* sanction (against thieves or trespassers), while much of information security relies on *ex ante* exclusion through encryption or access controls. The worse *ex ante* security is, the more costly and developed the *ex post* system for recovering the assets must be.

As a result of property's traditionally limited *ex ante* security, much law is concerned with making sure that unauthorized transfers do not threaten the information that possession of property conveys to third parties. For example, property law strongly sanctions unpermitted possession. It is not clear, without more, why it should do so—unpermitted possession does the property no harm. One likely answer is that possession is a powerful information rule.[247] The fact of possession conveys information so powerful that the person possessing property is considered its owner for the purposes of all but a very few interactions, which are based on some superior information source (say, being pulled over by police who have run the plates).[248] The best way to steal property is to hack the property system by impermissibly obtaining possession, thereby broadcasting ownership to the majority of people who encounter the thief

246. Of course, locks and safes exist, but they weaken a key feature of property, which is the ability to use the goods openly without having someone take them. Property that cannot be used while being locked up is not much good as property.

247. Carol M. Rose, *Possession as the Origin of Property*, 52 U. CHI. L. REV. 73, 78–79 (1985). *See also* Smith, *The Language of Property*, *supra* note 196, at 1117–19 (discussing different possessory rules and the informational content they provide to different audiences); Merrill & Smith, *Property/Contract*, *supra* note 196, at 803 ("[S]ubstantive legal norms associated with in rem rights are more likely to be expressed as rules that turn on one or a small number of publicly observable states of fact . . . . The common law rule that the person in possession of a resource is presumed to have a property right is one example.").

248. *See* sources cited *supra* note 247.

with the property. Thus, law sanctions unpermitted possession even if the property is unharmed and the owner has not yet missed the property.

Traditional property principles provide security for information assets as well. Consider domain names, which have been recognized by some courts as sharing some characteristics with traditional property. In *Kremen v. Cohen*,[249] Judge Kozinski wrote for the Ninth Circuit Court of Appeals:

> Property is a broad concept that includes "every intangible benefit and prerogative susceptible of possession or disposition." We apply a three-part test to determine whether a property right exists: "First, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity." Domain names satisfy each criterion.[250]

Kremen considered the theft of a domain name obtained by deceiving the centralized authority, then Network Solutions, Inc. ("NSI"), which maintained the register of domain name registrations.[251] Cohen exploited NSI's lack of security in the domain name ledger to illegitimately transfer the valuable domain name Sex.com.[252] His approach was low-tech social engineering. He sent forged letters and faxes from the original registrant claiming that the domain name had been abandoned.[253] The effect was a simple deletion of a claim on a registry. Once NSI had deleted the registration, Cohen snapped up the domain name.[254] The effect was to transfer a valuable intangible and rival property interest through the exploitation of a security loophole (here, NSI's employees' credulousness) by modifying the ledger. The Ninth Circuit held that the district court should not have rejected Kremen's claim for conversion, and remanded. In so doing, it applied entirely ordinary property rules to a ledger registration change.[255]

While traditional *ex post* property sanctions can protect digital property, new information security measures, such as advances in public

249. Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003).

250. *Id.* at 1030 (citations omitted).

251. *Id.* at 1026–27. *Kremen* also considered the potential liability of NSI for its failure to prevent Cohen from taking the Sex.com domain name. *Id.* at 1028–29. This part of the decision, bearing as it does on an Internet intermediary's responsibility to undertake expensive verification for a cheap service, is more controversial, and is not touched upon here except to note that decentralized public trustless ledgers ameliorate this problem by reducing the role of intermediaries.

252. *Id.* at 1026–27.

253. *Id.*

254. *Id.*

255. *Id.* at 1036.

ledgers and encryption, can also protect physical property. Consider smart property: property that is enhanced with embedded software, and perhaps further secured by linking the software to a slot on a block chain.[256] Smart property (at least in the sense of software-embedded and networked property) is becoming the norm for objects usually considered traditional personal property. Cars, houses, glasses, and watches are rapidly joining smart phones and tablets as being primarily protected by software control. A smart car linked to the block chain might "know," for example, that it is owned by the owner of a specific ledger entry, and will only start in the presence of the person to whom that ledger entry is ascribed. Keys cannot be duplicated because the slots on the ledger are rivalrous. The same public-key encryption infrastructure that has long secured information can now secure physical property against theft.

In sum, this part has argued that the conceptual core of property is not tangible things, not identity, and not sticks from the bundle, but information. As information, property is formatted, transferred, verified, and stored through a variety of protocols that share the virtues of good information transfer protocols. The rules of property set strong data formats, verify data, clear errors, and store information securely against manipulation or theft. Viewing property in this way paves the way for an actual operational digital property system. The following part offers suggestions for how to use trustless public ledger technologies to build such a system, as well as addressing challenges to the view of property espoused here.

III. OPERATIONALIZING BITPROPERTY

The preceding parts have described a potentially disruptive technology for tracking peer-to-peer and decentralized ownership interests, and have shown how such technology lays bare the nature of property as information. This part offers specific suggestions for how to clear away conceptual rubble in order to build a working system of digital property, and addresses potential conceptual challenges to the approach offered above.

A. NECESSARY ADJUSTMENTS TO CURRENT THEORY

A theory of property as information complements existing conceptions of property. Under a theory of property as information, the identity of the owner, attributes of the asset, or the nature of the relationship are just data

256. Ethereum, *supra* note 94, at 5:33.

to be formatted, transferred, verified, stored, and secured by a given property system. The property protocol does not dictate the goal of the system or transaction, whether that goal be efficiency, productivity, ensuring maximum exploitation of resources, or self-actualization. There is therefore very little tension, and in fact significant synergy, between other accounts of property and an information-based approach.

Nevertheless, there are some inconsistencies between some views of property and a theory of property as information. Property-as-information is inconsistent with the contention that legal categorizations in property should have anything to do with physicality. For property-as-information to take hold as an operative legal theory, property theory must dispense with physicality (or, conversely, intangibility) as the characteristic used to sort asset categories, and replace it with an analysis of rivalrousness and scarcity. Practically speaking, this will mean a rebalancing and reduction of the role that intellectual property has played in the online ecosystem. This section addresses each in turn.

1. Disentangling Tangibility

There are significant conceptual obstacles in the law of property, which if unchecked will substantially impede the cost and security gains made possible by trustless digital architectures. The first and most significant of these is the role that tangibility plays in courts' characterization of assets. As Juliet Moringiello notes, tangibility has long stood as a bad proxy for rivalrousness.[257] Block chain technology provides strong practical evidence against the notion that intangible assets cannot be rivalrous. The law of property must definitively abandon the connection between tangibility and rivalrousness if property law is to survive the transition to online contexts.[258]

Tangibility is a bad proxy because it is both imprecise and unnecessary. Tangibility stands in for two distinct variables, scarcity and rivalrousness. Scarcity is a function of supply and demand. If there is more of a thing than people who want it, it is not scarce. Rivalrousness is a measure of exclusivity of possession. If person A holds a rivalrous

257. *See* Moringiello, *False Categories*, *supra* note 2, at 137 ("Despite the fact that individuals commonly think of intangible rights embodied in almost worthless tangible things as property, intangible rights unconnected to tangible things continue to confound judges.").

258. *Id.* at 120, 140 ("[T]he category of 'tangible' is irrelevant in property law and . . . commercial law must discard distinctions based on the physical manifestations of assets and focus instead on the legal qualities of those assets . . . . This habit is a harmful one because it directs judges and lawmakers to look to intellectual property law rather than property law generally for rules to govern electronic assets.").

resource, person B does not. Physical resources can be scarce, rival, neither, or both. Air, for example, is physical, but neither scarce nor rival. A rock is rival but not scarce. A chance to hear Joshua Bell play in the Washington metro is scarce but not rival.[259] A gemstone or a bitcoin is both.

Tangibility is therefore a bad substitute for scarcity and rivalry. An asset may be rival and tangible, in the form of traditional personal property. An asset may be intangible and non-rival, in the form of traditional intellectual property. An asset may be intangible, rival, and scarce, as are bitcoins. Or an asset may be intangible, rival, and non-scarce, as would be entries in a non-capped public ledger. As the following subpart will demonstrate, when courts fail to make precise distinctions about scarcity and rivalry, and instead rely on the crude proxy of physicality, they both wrongly apply intellectual property protections to non-intellectual property intangible assets, and deny the protections of basic property law to the owners of such digital objects.

2. Differentiating Digital and Intellectual Property

One of the most marked difficulties in the development of online commerce has been the failure to develop a distinct theory of digital property that can withstand the incursions of intellectual property law.[260] The result is that many consumers own practically nothing online. Where they once owned bookcases full of books, consumers now have limited access to accounts with Amazon Kindle that can be erased at the whim of the copyright holder.[261] Where consumers once had record or CD collections, they now have nothing upon ending a relationship with a music streaming service.

There are both legal and technological aspects to this failure. The technological infrastructure of e-commerce has grown up around an ostensible truth of online assets: that because there is supposedly no way to prevent duplication of digital assets, any digital rights system must rely on a centralized list and list-verification authority to keep track of who may access which content. Legally, this centralization was accomplished

259. Gene Weingarten, *Pearls Before Breakfast*, WASH. POST (Apr. 8, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/04/04/AR2007040401721.html/.

260. *See* Moringiello, *False Categories*, *supra* note 2, at 141 ("[C]ourts and some scholars tend to give new intangible rights the 'intellectual property' label.").

261. Brad Stone, *Amazon Erases Orwell Books from Kindle*, N.Y. TIMES (July 17, 2009), http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html.

through intellectual property rules.[262] A central list curator can hold the copyrights and issue limited licenses to consumers. This creates a hub-and-spokes legal framework that fits the perceived need to create and verify a centrally maintained list. Given that decentralized ledgers of rival, non-duplicable interests are practicable, it is time to reexamine whether intellectual property remains the best governing law for non-intellectual property interests in discrete and rival digital objects.

Consider an MP3 track. If the track resides on a compact disc, it is considered tangible, and its owner gains certain rights from possessing the physical disc—for example, the ability to resell the specific copy under the first sale doctrine.[263] Yet if that track resides on the cloud,[264] its intangibility is construed by courts as presenting the possibility of infinite forward copying, the ultimate non-rivalrousness.[265] It does not matter much to courts that the MP3 on the CD could be copied forward, nor does it appear to matter under current doctrine if an MP3 residing on the cloud were not susceptible to forward copying.

This debate about rivalrousness and intangibility of digital goods is currently shaping the next generation of Internet startups and technologies. For example, *Capitol Records v. ReDigi*[266] examined whether an online marketplace committed primary and secondary copyright infringement for aiding customers in reselling their used MP3 files.[267] ReDigi, the defendant, attempted to create a market for used MP3s by deleting each copy as it was being migrated for sale or transfer to ReDigi's cloud service.[268] By dint of deletion-upon-migration, ReDigi achieved a crude but

262. *See id.*

263. *See* UMG Recordings, Inc. v. Augusto, 628 F.3d 1175, 1183 (9th Cir. 2011) (concluding that UMG's distribution of promotional CDs transferred ownership of those copies to their recipients, such that further sale of those copies was permissible under the first sale doctrine).

264. *See* Peter Mell & Timothy Grance, NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf ("Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.").

265. *See* Capitol Records, LLC v. ReDigi, Inc., 934 F. Supp. 2d 640, 656 (S.D.N.Y. 2013) ("Time, space, effort and cost no longer act as barriers to the movement of copies, since digital copies can be transmitted nearly instantaneously anywhere in the world with minimal effort and negligible cost. The need to transport physical copies of works, which acts as a natural brake on the effect of resales on the copyright owner's market, no longer exists in the realm of digital transmissions." (quoting U.S. COPYRIGHT OFFICE, LIBRARY OF CONG., DMCA SECTION 104 REPORT 82–83 (2001), *available at* http://www.copyright.gov/reports/studies/dmca/sec-104-report-vol-1.pdf)).

266. *ReDigi*, 934 F. Supp. 2d at 640.

267. *Id.* at 648–52.

268. *Id.* at 645.

functional form of rivalrousness.

To use the ReDigi market, consumers were required to download a local client.[269] That client then ensured that any file that was uploaded to the ReDigi marketplace was deleted from the local hard drive. The local client also scanned the computer for illicit attempts to retain a copy of the sold file.[270] The upload process used by ReDigi ensured that only one copy of the file was ever in existence before, during, or after upload for resale.[271] Once the song was uploaded to ReDigi's cloud service, it could be resold without copying by merely changing which user had access to the uploaded copies.[272] These elaborate precautions were necessary because the law of copyright posed a significant threat to the ability of a user to transfer their particular ownership in a single copy. This, indeed, was the result of the decision: the *ReDigi* court determined that a transfer of a digital object across the Internet could not be accomplished without creating a new and infringing copy.[273] The court interpreted intellectual property law to ban an emerging technology that attempted to create discrete, rival rights in intangible assets.

Particularly telling was the *ReDigi* court's reliance on a United States Copyright Office report, which took express note of the debate over whether so-called "forward and delete" methods could create rival digital objects subject to traditional property rules.[274] The report noted:

> Additionally, unless a "forward-and-delete" technology is employed to automatically delete the sender's copy, the deletion of a work requires an additional affirmative act on the part of the sender subsequent to the transmission. This act is difficult to prove or disprove, as is a person's claim to have transmitted only a single copy, thereby raising complex evidentiary concerns. There were conflicting views on whether effective forward and delete technologies exist today. Even if they do, it is not clear that the market will bear the cost of an expensive technological measure.[275]

To the Copyright Office and the courts, the problem of copying intangibles appeared insoluble with then-extant technology. Courts therefore resolved the question in favor of copyright holders, forcing digital

269. *Id.*
270. *Id.* at 645–46.
271. *Id.*
272. *Id.*
273. *Id.* at 651.
274. *Id.* at 655–56 (discussing how the Digital Millennium Copyright Act impacts distribution of digital works).
275. http://U.S. COPYRIGHT OFFICE, *supra* note 265, at xix.

assets back into the intellectual property mold. Yet even if the Copyright Office's determination were correct at the time, it has been overtaken by technological development.

The Copyright Office was concerned about copying and cost. Both concerns can be ameliorated by cryptologically sound ledgers. As above, duplication and double spending are two sides of the same coin. A user can no more spend a token in a block chain and keep it than she can give it to two different entities. Imagine a system in which the token acts as a key, permitting access to music streamed from a server. In this way, the music would not be duplicated by passing on the key to another user, permitting transfer without copying. While this form of duplication protection is not perfect, it does provide superior security to current solutions, at significantly lower cost. The technology outcompetes (especially on price) centralized technological measures such as rootkits, license servers, and other DRM traditionally employed by copyright holders. Thus, the cost prediction of the Copyright Office was incorrect. Block chain based ledgers strongly resist falsification, duplication, and double spending, and they do so at a cost low enough to support very high volume, low value transactions.[276]

One can read cases like *ReDigi* as merely demonstrating judicial caution in the face of developing technology. Yet the concept of tangibility continues to exert influence across the board. For example, in a range of cases construing when a product developer may access computer code to build a product that is interoperable with another, the cases align nearly perfectly along the tangibility/intangibility axis. If a business wants to manufacture a universal garage door opener or television remote or refillable ink cartridge that avoids a printer manufacturer's software restrictions, it may do so.[277] If the product is entirely intangible, a combination of contractual restrictions, licensing rights, and the Digital Millennium Copyright Act ("DMCA") can stop its development.[278] The development of new digital products and services requires that intellectual property make room for traditional ownership rights online without the physicality hook that has traditionally been required.

276. Jerry Brito, Houman Shadab & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 149–50 (2014).

277. Molly Torsen, Note, *Lexmark, Watermarks, Skylink and Marketplaces: Misuse and Misperception of the Digital Millennium Copyright Act's Anticircumvention Provision*, 4 CHI.-KENT J. INTELL. PROP. 117, 120–22 (2004).

278. *See* Davidson & Assocs. v. Jung, 422 F.3d 630, 637, 641–42 (8th Cir. 2005) (holding that a game developer whose employee clicked on a license agreement agreed to forego DMCA interoperability and reverse engineering protections).

3. Establishing Block Chain Neutrality

The prior two subparts have discussed problems within the common law (which prefers tangibility) and statutory framework (which overemphasizes intellectual property) that stand in the way of an operational digital property system. This subpart clears similar conceptual rubble from the perspective of potential regulators. This Article has attempted to demonstrate that trustless public ledgers can be put to a range of quite different uses. The danger is that block chain technologies as a whole may be cabined to one use case by the development of a specific legal regime, say, payments and money transmission services, and not left open to other potential uses.

Block chain technology should be regulated based on how it is being used, not on an attempt to determine what the technology is. Multiple, completely separate use cases can coexist side-by-side on a single block chain. The block chain is neutral. It is simply a protocol for tracking information about rivalrous digital interests that provides a strong solution to the duplication problem without requiring a central curating authority.

From the perspective of financial crimes enforcement, general law enforcement, and anti-money laundering or counter-threat-finance efforts, cryptocurrencies are a barely tolerable innovation because the technology can be used to transfer value among criminals.[279] Under this view, regulators will work to reduce the fluidity and pseudonymity of trustless property systems. This is in response to many news stories describing the use of Bitcoin to purchase drugs, guns, or pornography.[280] The approach is tinged with some new-technology hysteria, but has a serious point. There is no question that cryptocurrencies, like cash, will facilitate bad acts. The question is whether a ban or highly constraining regulation will do more harm than good.[281]

There is a growing consensus that block chain technologies will be regulated.[282] A multi-voiced discussion among regulating entities, industry,

279. *See* Laurie Law, Susan Sabett & Jerry Solinas, *How to Make a Mint: The Cryptography of Anonymous Electronic Cash*, 46 AM. U. L. REV. 1131, 1136–37 (1997) (noting that the free transferability of money may facilitate crime).

280. *See, e.g.*, Andy Greenberg, *Follow the Bitcoins: How We Got Busted Buying Drugs on Silk Road's Black Market*, FORBES (Sept. 5, 2013, 10:36 AM), http://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/ (highlighting a study which found that 295,435 out of over a million identified Bitcoin transactions had drug market ties).

281. *See* Kaplanov, *supra* note 5, at 167 (noting that there is "some interest in trying to limit or ban bitcoins").

282. Zachary Warmbrodt, *Bitcoin Gets Ready for the Government*, POLITICO (Nov. 14, 2013, 4:59

consumer protection advocates, and legal academics is already taking shape.[283] There is a strong case for careful regulation: almost all use cases for trustless technology stem from permitting people to trade something of value. Indeed, that is the purpose of trustless technology. Trading things of no value does not require a trustless system, since there is no problem of trust.

Wise regulation of trustless technologies will take note of the multiple different use cases to which the technology can be put. It will avoid applying financial regulatory rules to startups that use the Bitcoin block chain for non-financial purposes. It will discriminate between value transfer systems, like property transfer registries, and financial use cases, like cryptocurrencies. It will sharply define the limits of rules that do cover financial use cases, so as to not impinge on co-extant non-currency uses. Finally, wise regulators will rapidly reevaluate and update rules as new use cases emerge. Although these updates will sacrifice some certainty, a humble, iterative, experimental approach to regulation will permit entrepreneurs to explore the technology for potential breakthrough uses.

B. CONCEPTUAL CHALLENGES

Whereas the prior section laid out pragmatic changes in the law that will be necessary to operationalize a true digital property system, this section will address conceptual counterarguments that challenge the theory advanced above. As proposed above, the essence of property is not things, not identity, not relationships, not sticks from the bundle, but information. As a corollary, property systems are information transfer and storage protocols. To this theory one might address several related criticisms, with which this section engages.

1. Is Information Separate from Property?

A critic might first argue that while information about property is important, and while it should be communicated through secure networks and stored in secure facilities, this does not provide any support for the idea that the heart of property is information.[284] The critic might strongly

PM), http://www.politico.com/story/2013/11/bitcoin-gets-ready-for-the-government -99893.html.

283. Sydney Ember, *New York Proposes First State Regulations for Bitcoin*, N.Y. TIMES (July 17, 2014, 3:01 PM), http://dealbook.nytimes.com/2014/07/17/lawsky-proposes-first-state-regulations-for-bitcoin/. *See also* sources cited *supra* notes 281–282.

284. *See, e.g.*, Timothy P. Terrell, "*Property," "Due Process," and the Distinction Between Definition and Theory in Legal Analysis*, 70 GEO. L.J. 861, 865–74 (1982) (suggesting that the essence of property is made up of the following three entitlements: the rights of exclusion, powers of transfer, and privileges of use).

differentiate between information about property and property itself. This conceptual move might be accompanied by a strong distinction between a physical, tangible thing and information about that thing.

The proposition that property law sets up an information protocol does not merely concern information about property.[285] Rather, the flow of property interests is itself information that percolates through human systems. Consider a fictitious tribe with an economy based on trades in shells.[286] Those shells carry information, not just about the shells themselves, but about the goods and services one can command with those shells. The allocation of shells serves as a history of transactions. The shells serve as a social memory of all past deals.[287] One might replace the shell system with a system in which an elder of the tribe with perfect recall must witness all transactions—that is, the shells serve as a substitute for a system in which there is perfect memory.[288] In short, the property system and the information system are interchangeable. They are the same thing. Property is a way of recording the state of resource distribution in a society.[289] It is not a catalog of all resources, but an information system designed to record the distributional decisions by which all members of the society are bound. Cash in a wallet is as much a record of resources at an individual's disposal as is an entry in a bank account. Similarly, possession and ownership of a car serves as a record of the history of transactions that has caused that particular group of components to be assembled and brought to the point where it is parked in someone's driveway and at their disposition. Property itself, its location, amount, possession and use, is thus an information system recording the current state of social resource allocation. Like the movement of beads of an abacus, the movement of property is itself information.

2. Is Information Subordinate to Property?

Another potential contention might be that information is important to property, but is subordinate to some other characteristic. For example, a

285. Although such information plays a significant part and is, under this theory, at least some of the information that must be transferred.

286. *See* William J. Luther & Josiah Olson, *Bitcoin is Memory*, 3 J. PRICES & MARKETS 22, 23 (2015) (discussing the relationship between money and memory); Narayana Kocherlakota & Neil Wallace, *Incomplete Record-Keeping and Optimal Payment Arrangements*, 81 J. ECON. THEORY 272, 273 (1998) (discussing money as an imperfect memory-keeping device); Narayana R. Kocherlakota, *Money is Memory*, 81 J. ECON. THEORY 232, 233 (1998) (describing the movement of money as a method of storing information about resources).

287. *See* sources cited *supra* note 286.

288. *See* Luther & Olson, *supra* note 286.

289. *See* sources cited *supra* note 286.

critic might note that records—information—do not constitute definitive proof of ownership in many jurisdictions. If the record is proven to be incorrect, the "true" owner will prevail. One might conclude from this that information is subordinate to some other characteristic of property, and that the property interest does not reside in the data, but in some other feature of the thing itself, the transaction, or the relationship of the parties.

This criticism significantly underestimates the primacy of information in property. A record of property ownership is only overturned on better information—better data—about who ought to be considered the actual owner. That is, there is no true, absolute owner. There is only the owner indicated by the best information that the legal system can access. While it is true that information about ownership stored in land records and verified by the procedures of the clerk's office can be trumped by information stored in human minds (testimony) and verified by the procedures of the court during litigation, the question remains one of information. The owner is the entity to whom the best information points. The property right resides in the information.

A similar challenge might arise from transfers of property by secret deed or private delivery of a gift. In such a transfer, the information about the transfer is not available to third parties, yet law seems to recognize the transfer. If property is an information transfer protocol, a critic might reasonably ask, how can it be that the legal system treats secret property transfers as valid? A response might be that the property right propagates as a function of information propagation. Consider information as ripples in a pond, spreading from the point of origin. As between the transferor and transferee, the secret transfer is effective. Consider again C, a non-party to the transaction, who learns about it from A or B. C promptly loses bona fide purchaser status upon hearing of the transfer. Wherever the information flows, it shifts the relationship of the parties with respect to one another and to the asset.

3. Is All Information Property?

A final contention might be that conceptualizing property as information presses too far and implies that because property is a kind of information, all information is property. Such a criticism would, if correct, raise serious cause for concern with advocates for less propertization of information and for more access to knowledge. But the criticism would be inapt. Property is merely one kind of information system. All information cannot and should not be made into property, and that is not the contention of this piece. On the contrary, the approach suggested here demonstrates that property is a special subcategory of information. Property is the subset of information systems that record transferrable, scarce, rival, persistent, and sharply delineated data objects. This holds for transfers of real estate, personal property, smart property, and digital property. Consider, for example, a proposed transaction in which someone wishes to sell a digital object—a bitcoin, a digital magic sword in a game, or a used MP3. A buyer will want to know whether the object is transferrable (Can the buyer actually obtain it from the seller?), persistent (Will it hold value?), rival (Can the seller retain a copy and resell it?), scarce (How hard is it for the buyer to obtain her own?), and sharply delineated (Are there clouds on title? Is there lack of clarity as to whether the asset is being bought or licensed?). Most information does not possess the characteristics of transferability, persistence, rivalry, scarcity, or delineation that are necessary for digital property rights. Such information should not be considered property.

While all information is not property, all property is information. There is an important balance. Courts must not propertize non-rival and non-scarce information resources outside of the confines of the intellectual property system. Yet they must also learn to apply traditional property rules to scarce and rival intangible resources. There will be significant difficulty in finding the right balancing point and in calling close cases. Rivalry and scarcity are continuous, not discrete, variables. Assets can be more or less scarce, and more or less rivalrous. While easy cases like Bitcoin will fit smoothly into the law of property because of their clear scarcity and rivalry, hard cases will arise at whatever balancing point courts select. The existence of hard cases should not prevent courts from recognizing decentralized, rival, and scarce digital property interests.

CONCLUSION

Ledgers are the backbone of modern and sophisticated property systems. Such systems must keep track of millions of transactions worth trillions of dollars, must be kept up to date, must be accurate, and must be low-cost to maintain. Until recently, accomplishing this task without a centralized and trusted authority was not practical. As a result, property ledgers are split up among different verification authorities. They are hard to access, difficult to reach and search, and comparatively easy to manipulate or compromise.

Block chain technologies promise significant gains in efficiency, certainty, and security over traditional methods of creating and tracking legal rights. They offer the possibility of decentralized and secure ledgers to maintain digital property, currency, county land records, mortgage interests, security interests, stock ownership, and much more. Trustless public ledgers track transactions in real time, at comparatively low cost. The fact that ledgers are public means that they are available to anyone to track the flow of interests, permitting users to manage risk and monitor exposure. In online ecosystems, transaction costs are everything. The inability to track property interests cheaply has meant that property law has not yet come into its own online. With the advent of block chain technology, there is a serious chance it may do so.

The invention of a decentralized property technology for intangibles offers an opportunity to reflect on the tortured history and uncertain future of digital property. Unlike electronic contracts or cybertorts, digital property is only now being born, after a long and hard labor. The core problem is that true digital rivalry and scarcity have been difficult to create, and the common law of property associates traditional property rules with tangible things rather than informationally compact data objects. As a result, courts have assumed that traditional property rules are simply inapplicable to online information-based resources, and have misapplied and overextended intellectual property law to fill the gap.

What is needed, and what this Article has attempted to provide, is a theory of property as information. Property is not merely a system for constraining information costs by limiting form choice and modularizing clearly delineated packages of rights in things. Property is a system for formatting, transmitting, verifying, and securely storing information tying together identities, rights, and resources. Such an approach not only permits significant improvements on currently extant information cost theory, but also directly confronts the pernicious view that traditional property has no place online. Once the conceptual blocks that have prevented the full bloom of digital property online have been cleared away, the common law can put the cost savings and scaling effects of networked communications technologies to work to create an operational system of digital property.