Minnesota Journal of Law, Science & Technology

Volume 19 | Issue 1 Article 2

2018

Blockchain's Struggle to Deliver Impersonal Exchange

Benito Arruñada
Universitat Pompeu Fabra

Blockchain's Struggle to Deliver Impersonal Exchange

Benito Arruñada*

The paper identifies what value blockchain adds to the contractual and property processes, exploring its potential and analyzing the main difficulties it is facing. It argues that, contrary to naive conceptions that proclaim the end of intermediaries and state involvement, blockchain applications will rely on a variety of interface, completion, and enforcement specialists, including standard public interventions, especially for property transactions. Without these interventions, blockchain applications will at most enable trade in in personam claims instead of in rem rights, therefore facilitating personal instead of truly impersonal—that is, asset-based—transactions.

Keywords: property rights, enforcement, transaction costs, impersonal exchange, blockchain, distributed ledgers, smart contracts.

JEL: D23, K11, K12, L85, G38, H41, O17, P48.

[*] Pompeu Fabra University and Barcelona GSE. E-mail: benito.arrunada@upf.edu. This work has greatly benefitted from exchanges with Fátima Antelo, Winston Featherly-Bean, Luis A. Gallego Fernández, Luis Garicano, Teófilo Hurtado Navarro, Eduardo J. Martínez García, Fernando P. Méndez González, Nicolás Nogueroles Peiró, Rod Thomas, Luis Torras, Jacques Voss, and participants at the World Bank Conference on Land & Poverty, the Annual Meeting of the American Law & Economics Association and the Annual Conference of the Society for Institutional & Organizational Economics, as well as the editorial assistance of Ian Todd. Several ideas were added while collaborating with Luis Garicano on a related project. It received support from the Spanish Ministry of the Economy and Competitiveness through grant ECO2014-57131-R and the Severo Ochoa Program for Centers of Excellence in R&D (SEV-2015-0563). Usual disclaimers apply.

I. INTRODUCTION

Blockchain—often known as "distributed ledger technology"—has been sold as the most important technological innovation in today's economy.[1] Even if it is difficult to separate substance from hype, it is clear that not only have thousands of blockchain applications been launched, but the biggest firms in many industries are investing substantial amounts of resources in blockchain-related efforts.[2] However, it is also becoming apparent that serious and recurrent difficulties are delaying, if not killing off, what for the time being are still modest applications of the technology.

This paper aims to ascertain the importance of blockchain and clarify both the development of blockchain applications and

[1] *See, e.g.*, U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 8 (2016) (claiming that blockchain technology "provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector.").

[2] Including the food, financial services, energy, pharmaceuticals, health, aerospace, aviation, telecommunications, IT and communications, transport, utilities, agriculture, and oil and gas industries. Simon Taylor, *Vision*, *in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 24. Based on a survey of 134 global market participants in capital markets, Greenwich Associates estimate that in 2016 financial service firms and technology providers spent more than one billion USD worldwide to adopt blockchain in capital markets alone. RICHARD JOHNSON, GREENWICH ASSOCS., BLOCKCHAIN ADOPTION IN CAPITAL MARKETS 6 (2016). The same study estimated in June 2016 that venture capital investment in blockchain technology had climbed to over 440 million USD. *Id.* at 3.

the necessary adaptive decisions to be made in business firms' strategies and legal institutions. After introducing the basics of blockchain and its most disruptive application (so-called smart contracts), the paper will explore the main challenges faced by blockchain applications. It will do so from the perspective of the economic analysis of property rights. It will therefore pay particular attention to, first, the legal distinction between contract (personal or in personam) rights and property (real or in rem) rights;[3] and, second, the related distinction between private and public legal "ordering."[4] As a consequence, the paper complements efforts to understand the economic effects of blockchain on transactions that in fact deal only with in personam rights.[5]

The analysis will be grounded on the theoretical and empirical premise that, while market participants can trade contract rights easily under private ordering arrangements based on reputational assets and the expectation of future trade, trading in in rem rights requires a minimum of public ordering—in particular, an enforcer who is neutral and independent not only of parties to a given contract but to all holders of property rights on the type of asset being traded in that market.[6]

In line with this premise, the paper will analyze how a common problem of some pioneer applications of blockchain lies in a tendency to overestimate the power of private ordering and to minimize that of trusted intermediaries, which has often led

[3] *See* Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1 (2000); Henry Hansmann & Reinier Kraakman, *Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights*, 31 J. LEGAL STUD. S373 (2002).

[4] *See* Benito Arruñada, *Coase and the Departure from Property*, *in* THE ELGAR COMPANION TO RONALD H. COASE 305 (Claude Ménard & Elodie Bertrand eds., 2016) [hereinafter Arruñada, *Coase and the Departure from Property*]; Benito Arruñada, *Property as Sequential Exchange: The Forgotten Limits of Private Contract*, 13 J. INSTITUTIONAL ECON. 753 (2017) [hereinafter Arruñada, *Property as Sequential Exchange*].

[5] *See, e.g.*, Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* (Nat'l Bureau of Econ. Research, Working Paper No. 22952, 2016), http://www.nber.org/papers/w22952.

[6] *See* BENITO ARRUÑADA, INSTITUTIONAL FOUNDATIONS OF IMPERSONAL EXCHANGE: THE THEORY AND POLICY OF CONTRACTUAL REGISTRIES 67–71 (2012) [hereinafter ARRUÑADA, INSTITUTIONAL FOUNDATIONS]; Arruñada, *Coase and the Departure from Property*, *supra* note 4; Arruñada, *Property as Sequential Exchange*, *supra* note 4.

to frustrated expectations.[7] This is not a new problem, however, as land titling and administrative simplification efforts have been suffering similar problems for the same reason.[8] Therefore, blockchain development can benefit greatly from borrowing insights from the critical analysis of the recurrent management and policy mistakes made in these areas. This is particularly so in property applications, as analyzed in Section 5.

II. A BRIEF ON BLOCKCHAIN AND "SMART CONTRACTS"

A. THE NATURE OF BLOCKCHAIN

Blockchain is the technology underpinning the bitcoin cryptocurrency.[9] As with any other type of money, electronic money must make sure that it changes hands without risk of being diverted and is not spent twice by the same individual.[10] Traditional payment systems solve these problems by relying on central, specialized, and trusted third parties such as banks, payment systems, credit card companies, and clearing houses.[11] In contrast, the blockchain solved them with a peer-to-peer solution.[12] It is capable of replacing the trusted third party because it contains the history of all previous transactions, so is a source of evidence for establishing who owns what at any given moment.[13] To achieve this feat, it replicates the ledger in a multitude of computers or "nodes," making all the history of

[7] *See infra* notes 106–112 and accompanying text.

[8] *See* Benito Arruñada, *Pitfalls to Avoid when Measuring the Institutional Environment: Is 'Doing Business' Damaging Business?*, 35 J. COMP. ECON. 729 (2007); Arruñada, *Property as Sequential Exchange*, *supra* note 4.

[9] *See, e.g.*, Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 577 (2015) ("[Blockchain] is the core innovation driving the bitcoin currency system.").

[10] *See, e.g.*, *id.* at 577 n.54.

[11] *See, e.g.*, Jeremy Clark, *Foreword* to ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION XI–XIII (2016).

[12] *See, e.g.*, Kiviat, *supra* note 9, at 580 (footnotes omitted) ("[B]lockchain establishes trust between two parties to a transaction through both a decentralized public ledger and a cryptographic mechanism that ensures transactions cannot be changed after the fact. One can easily see why the creator of this technology called it 'purely peer-to-peer . . . electronic cash.'").

[13] *See, e.g.*, *id.* at 578–79 (footnote omitted) ("[Blockchain] makes a collective accounting by distributing a shared (that is, decentralized) public ledger—a complete record of all past transactions on the network.").

transactions public, accessible, and widely distributed across the whole network of users.[14]

Moreover, before entering the ledger, transactions must achieve the consensus of the community, produced online by a mechanism in which the participants implicitly agree to change the blockchain.[15] Assume, for example, that *A* and *B* are members of the community of users. E.g., both have bitcoin "wallets," a type of software that accesses the Internet without identifying the owner (a paradigm of impersonality),[16] even if their personal identities are always protected by cryptography.

Assume also that *A* wants to transfer an asset (e.g., bitcoin money) to *B*. *A*'s wallet first proposes to change the blockchain to reduce *A*'s balance and correspondingly increase *B*'s balance. This proposal circulates around the network and participants are invited to confirm it by checking the ledger, which requires solving a complex cryptographic puzzle. Solving the puzzle demands plenty of computing power, as it must be done by trial and error. Some specialized users (called "miners") compete in solving it.[17] The system motivates these miners by paying them

[14] For a reliable introduction, see ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION (2016), its printed version will be quoted here, but its draft version is available at https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1. For detailed explanations, see the descriptions in Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 215–19 (2015); Trevor I. Kiviat, *supra* note 9, at 576–88; and Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 196–202 (2016). For the abundant literature that emphasizes blockchain's potential, see WILLIAM MOUGAYAR, THE BUSINESS BLOCKCHAIN: PROMISE, PRACTICE, AND APPLICATION OF THE NEXT INTERNET TECHNOLOGY (2016); DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD (2016). For a short introduction, see *The Great Chain of Being Sure About Things*, ECONOMIST, Oct. 31, 2015, at 19.

[15] *See* Böhme et al., *supra* note 14, at 217.

[16] *But see* Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters (detailing that this does not mean anonymity: "Much like email, which is quite traceable, Bitcoin is pseudonymous, not anonymous. Further, every transaction in the Bitcoin network is tracked and logged forever in the Bitcoin blockchain, or permanent record, available for all to see. As a result, Bitcoin is considerably easier for law enforcement to trace than cash, gold or diamonds.").

[17] NARAYANAN ET AL., *supra* note 14, at 124–30 (showing that for a long time now, most miners have been operating through "mining pools," sharing revenue according to the effort of each miner, which places the pool manager in

when they create a new block (e.g., twenty-five bitcoin or around 16,387 USD as of the date of this writing). The lucky miner is paid after other miners confirm the solution (which is an easy task). Only then is the new block added to the blockchain. In sum, the ledger is distributed in thousands of computers and the final version is the one accepted by a majority of computers.[18]

The system is protected against tampering and revision by duplication of the blockchain in many computers and concatenation of any subsequent blocks,[19] which makes it trivially easy to verify that the whole content of the chain has not been altered. The abovementioned puzzle refers to each block's "header" that contains a "hash" produced by a cryptographic function, plus some other data specific to the block (e.g., each block contains a timestamp and a link to a previous block).[20] The header is easy to produce on the basis of the information in the chain.[21] Therefore, if the chain's contents were modified, the change would cause an easily observable discrepancy, and the latest block would be rejected.[22]

Cheating is made even harder by the fact that it is not possible to predict which specific miner will solve the puzzle. Moreover, no miner can manipulate the chain because participants work on the longest chain. By the time a miner (imagine an *A* who wants to pay *B*) has been able to manipulate it, other participants would already be working on an alternative blockchain.[23] Therefore, a malevolent *A* would need to lengthen

a strong position, potentially reaching high levels of mining concentration. Even if their market shares have been fluid, real concentration is unknown because large miners can participate simultaneously in several pools (a practice known as "laundering hashes")).

[18] *See* Vitalik Buterin, *The Meaning of Decentralization*, MEDIUM (Feb. 6, 2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (distinguishing between architectural (how many computers can break down?), political (how many people ultimately control the computers?), and logical (if the system is cut in half, will both halves continue operating?) decentralization by stating "[b]lockchains are politically decentralized (no one controls them) and architecturally decentralized (no infrastructural central point of failure) but they are logically centralized (there is one commonly agreed state and the system *behaves* like a single computer)").

[19] *See* Matthew C. Stephenson, *Information Acquisition and Institutional Design*, 124 HARV. L. REV. 1422, 1462–75 (2011) (detailing the potential benefits of the costly solution of having redundant repositories of information).

[20] *See The Great Chain of Being Sure About Things*, *supra* note 14.

[21] *Id.*

[22] *Id.*

[23] *Id.*

the chain faster than all other users, which in principle would require *A* to control more than half of the network's computers.[24]

B. SMART CONTRACTS

Blockchain applications have been expanded by embedding information in the ledger, potentially including in it all steps in the contractual process, from ensuring the reliable recording and archiving of data to transferring all types of assets.[25] Therefore, blockchain technology is now applicable not only to payments but to all sorts of contracts; thus, instead of exchanging digital tokens valuable by themselves and existing only in the ledger (such as Bitcoin), parties can exchange representations of claims in all types of physical or digital assets existing outside the ledger.

[24] *See generally* JOSHUA A. KROLL, IAN C. DAVEY, & EDWARD W. FELTEN, THE ECONOMICS OF BITCOIN MINING, OR BITCOIN IN THE PRESENCE OF ADVERSARIES, 1 (2013), http://www.econinfosec.org/archive/weis2013/papers /KrollDaveyFeltenWEIS2013.pdf (including an analysis of the different equilibria of bitcoin participants and the security risks they pose. On this basis, they "argue that Bitcoin will require the emergence of governance structures, contrary to the commonly held view in the Bitcoin community that the currency is ungovernable."); MAGNUS KEMPE, THE LAND REGISTRY IN THE BLOCKCHAIN 34 (July 2016) (proposing development steps for the future).

[25] *See, e.g.*, BLOCKSTACK, https://blockstack.org/ (last visited Oct. 24, 2017) (showing how Blockstack allows registration of identities, public keys and names in the blockchain, providing more security than traditional identity, naming, and digital registries); COINSPARK, http://coinspark.org/ (last visited Oct. 24, 2017) (detailing how CoinSpark allows messages and assets to be added to bitcoin transactions, allegedly making it possible to "transfer any asset over the Internet" and "notarize important emails on the blockchain"); COLU, https://www.colu.com/ (last visited Oct. 24, 2017) (claiming to provide a tool for creating local economies, including the issuance of digital currencies); EVERLEDGER, http://www.everledger.io/ (last visited Oct. 24, 2017) (showing how Everledger is implementing a fraud-prevention registry of luxury goods such as diamonds, which, by recording their distinguishing attributes, would help provide proof of identity in case of theft); FACTOM, https://www.factom.com (last visited Oct. 24, 2017) (showing Factom tried to provide a prototype of land registry based on the blockchain to the Honduras' Property Institute). *But see* KEMPE, *supra* note 24, at 11–12, 15 (showing that it is the unique cryptographic hashes, which serve as verification records, and not the transaction documents, that are saved in the blockchain (consequently, this is another source of duplication, as two separate systems are kept in place to preserve both documents and hashes). The documents can be saved by many other parties, including parties to the affected transactions. This replication plus the set of verification records —also duplicated in the blockchain— guarantee that their integrity is preserved). *See generally* TAPSCOTT & TAPSCOTT, *supra* note 14, at 115–44 (detailing a general view of blockchain's applications).

One of its most ambitious applications is implementing the decentralized "smart contracts" first proposed by Nick Szabo, which feature automatic execution: they contain a set of rules that trigger predefined responses corresponding to particular contingencies.[26] (Vending machines, video-on-demand, and ATMs could be seen as simplistic antecedents. Multiple initiatives have been developing to implement smart contracts, from the very simple to the most complex.)[27] In a way, they use the blockchain ledger as their enforcement mechanism,[28] so that transactions are supposed to be conclusive or "immutable."

[26] Nick Szabo, *The Idea of Smart Contracts*, MANUSCRIPT (1997) http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/securetitle.html (last visited Aug. 1, 2016). The term, "smart contract" was seemingly first used by Nick Szabo:

> Many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher. A canonical real-life example, which we might consider to be the primitive ancestor of smart contracts, is the humble vending machine. Within a limited amount of potential loss (the amount in the till should be less than the cost of breaching the mechanism), the machine takes in coins, and via a simple mechanism, which makes a freshman computer science problem in design with finite automata, dispense change and product according to the displayed price. The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.

Id. See also Nick Szabo, *Secure Property Titles with Owner Authority*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html (last visited Aug. 10, 2016).

[27] *See* Jamie Burke, *99% of Blockchain Startups Are Bullshit*, MEDIUM (Mar. 17, 2017), https://convergence.vc/99-of-blockchain-startups-are-bullshit-4cf11a549895 (showing that, in fact, most smart contracts are quite dumb: "It's often very simple if-this-then-that"). For instance, payment to miners adding a block is deferred until 99 more blocks have been added to the chain. Similarly, decentralized crowdfunding services automatically go ahead only with projects that receive enough funding. *See, e.g.*, LIGHTHOUSE PARTNERS, http://www.lighthouse-partners.com/ (last visited Aug. 18, 2016).

[28] Kiviat, *supra* note 9, at 603–05 (stating that decentralized smart contracts are understood as "contracts that leverage a secure public ledger as an enforcement mechanism"). The basis of smart contracts is that they add conditions to the simple set of instructions ("script") of a bitcoin transaction, which consists of only three parts: "(1) Party A sends a message to the network declaring the transaction; (2) Party B accepts the transaction by broadcasting its acceptance; and (3) the network participants verify the transaction's

Understandably, the blockchain is often defined as a "trust machine" because it, supposedly, "lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority. Simply put, it is a machine for creating trust."[29] In this vein, some authors argue that smart contracts are such a fundamental innovation in the way transactions are organized and the scope for their application is so wide that they threaten the position of all sorts of intermediaries that provide trust or overcome the lack of trust between traders, including, most prominently, the role of lawyers.[30] However, smart contracts are subject to serious

authenticity." *Id.* Added conditions could reflect the parties' desire that the transaction occur only under certain circumstances or at a certain time, etc. *Id.*

[29] *The Trust Machine*, ECONOMIST (Oct. 31, 2015) (also stating that "[t]he blockchain . . . [i]n essence . . . is a shared, trusted, public ledger that everyone can inspect, but which no single user controls. The participants in a blockchain system collectively keep the ledger up to date: it can be amended only according to strict rules and by general agreement," and "[t]he real innovation [behind bitcoin] is not the digital coins themselves, but the trust machine that mints them—and which promises much more besides."). *But see* NARAYANAN ET AL., *supra* note 14, at 280 (emphasis added) (showing how complementary reliance on trusted components is necessary for achieving *security*, the real objective and a much less ambiguous term than *trust*, which is only one of the means to achieve it and stating that "'Trust minimization' is a worthwhile goal in the sense that *other things being equal*, we want to build systems with fewer components that we're reliant on for security. But when you have a hammer, everything looks like a nail, and Bitcoin enthusiasts often get carried away with removing trusted components from systems. A trusted component is not always bad, and the existence of a real-world trust relationship is certainly not a problem by itself.").

As we will see below, the applications make ample use of intermediaries acting as "trusted components."

[30] For example, a major Australian law firm concludes:

> At this stage, we aren't convinced that "smart contracts" will replace lawyers altogether. Currently, most use cases for smart contracts involve the execution of relatively simply contractual instructions or control functions. Some of the real advantages of smart contracts arise in the context of low value payments, which would cost more to enforce than the value of the transactions. For a smart contract to work effectively, the parties to a transaction need to be able to precisely define an outcome to make it the subject of code. The more complicated the provision or relationship, the more difficult it will be to code. However, it is likely that over time, smart contracts will apply to increasingly complicated situations, and be used for different purposes beyond simple commercial transactions.

ALLENS LINKLATERS, BLOCKCHAIN REACTION: UNDERSTANDING THE OPPORTUNITIES AND NAVIGATING THE LEGAL FRAMEWORKS OF DISTRIBUTED LEDGER TECHNOLOGY AND BLOCKCHAIN 15 (2016) (emphasis added), http://www.allens.com.au/data/blockchain/index.htm?sku=fsdah5e556eqweqwg.

limitations. As we will see below, once we move away from extremely simple transactions, it is necessary to consider a large number of possible contingencies, and this exponentially multiplies the difficulty of codifying the proper contractual outcomes. When envisioning these systems, we must avoid falling into the trap pointed out by Hayek with respect to economic planning:[31] scientific and statistical information is relatively easy to collect, aggregate, and transfer, but specific information includes "circumstances of time and place" that are well-nigh impossible to aggregate or transfer. Knowledge necessary for completing contracts often hinges on specific circumstances that cannot be easily standardized or conveyed. Moreover, automatic execution is costly to the extent that it would preclude efficient breach.[32]

III. BLOCKCHAIN AND CONTRACT, IN PERSONAM, RIGHTS

In principle, as explained above, the blockchain makes no use of specialized third parties for enforcement. It is not uncommon to find claims that blockchain or "DLTs [distributed ledger technologies] pose a threat to any hierarchical structure through an ability to connect and operate in a distributed

[31] *See* Friedrich A. Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519, 524 (1945) ("[T]he sort of knowledge with which I have been concerned is knowledge of the kind which by its nature cannot enter into statistics and therefore cannot be conveyed to any central authority in statistical form. The statistics which such a central authority would have to use would have to be arrived at precisely by abstracting from minor differences between the things, by lumping together, as resources of one kind, items which differ as regards location, quality, and other particulars, in a way which may be very significant for the specific decision. It follows from this that central planning based on statistical information by its nature cannot take direct account of these circumstances of time and place, and that the central planner will have to find some way or other in which the decisions depending on them can be left to the 'man on the spot.'").

[32] *See* ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 266 (5th ed. 2008) ("[G]iven costly renegotiations . . . the damage remedy for breach of contract has an advantage over specific performance, just as compensation has an advantage over injunction in nuisance cases with negotiation costs."). Law and economics has developed a whole subfield around the concepts of incomplete contracts and efficient breach. *See also* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 304–14 (2004) (analyzing remedies for breach of performance, including different type of damages and specific performance).

network, *without trusted or necessary intermediaries*."[33] In particular, smart contracts are supposed to work without third-party intervention, which theoretically avoids the risk of ledger manipulation by governments or other third parties. To this extent, smart contracts could, therefore, be understood as a paradigm of pure private ordering.[34]

In fact, however, blockchain applications require the intervention of between-parties intermediaries to write the code, run the system, and store data, in order to manage what can be seen as mere contract or in personam rights.[35] For instance, in addition to those making the rules,[36] blockchain applications

[33] Phil Godsiff, *Disruptive Potential*, *in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 61 (emphasis added); *see also* Fred Ehrsam, *How the Blockchain Could Change Corporate Structure*, WALL ST. J. (Oct. 19, 2016, 10:39 AM), http://www.wsj.com/articles/how-the-blockchain-could-change-corporate-structure-1476887998 ("[W]e will no longer need central companies to act as the middleman.").

[34] *Cf.* TAPSCOTT & TAPSCOTT, *supra* note 14, at 199–201 (showing blockchain has been considered by Libertarians as a means to get rid of the state altogether). However, a more nuanced view is in order. For instance:

> While a maximalist vision for decentralization might involve dismantling the state, this is not really [a] viable vision, especially when others who share our democracy want [a state]. However, decentralization through technology is not necessary in opposition to the state at all. In fact, they can be mutually beneficial. For example, assuming well-identified parties, transfers of smart property can use the block chain for efficient transfers and still use the court system if there is a dispute. We think the big opportunity for block-chain technology is implementing decentralization in a way that complement[s] the functions of the state, rather than seeking to replace them.

NARAYANAN ET AL., *supra* note 14, at 285.

[35] For an introduction to the distinction between property (in rem) and contract (in personam) rights, see Merrill & Smith, *supra* note 3; Hansmann & Kraakman, *supra* note 3. *See also* ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 15–34 (discussing the distinction's economic consequences); Arruñada, *Coase and the Departure from Property*, *supra* note 4, at 305–19 (discussing the distinction's economic consequences).

[36] Trust in a governing third party is required for the continued operation of blockchain applications. Rules need to be changed, and governance decisions are recurrently needed. This raises a paradox because:

> [O]nce you address the problem of governance, you no longer need blockchain; you can just as well use conventional technology that assumes a trusted central party to enforce the rules, because you're already trusting somebody (or some organization/process) to make the rules. . . . The differences to conventional technology are no longer that apparent. Perhaps blockchain technologies can still deliver better technical performance, like better availability and data integrity. But

may require other agents, such as "oracles," to monitor external or "off-blockchain" information for conditions that trigger contractual execution (e.g., whether the market price of oil reaches a certain level when that level is specified in a conditional clause of the contract), as well as "curators," to perform a variety of functions, including the pre-selection of application proposals and the prevention of attacks.[37] Even the dependence on oracles is thought to "undermine the goal of agreements free of human caprice."[38] And it is undeniable that curators add some degree of centralization and specialized enforcement.[39] Moreover, there are reasons to think that the

> it's not clear to me what real changes to economic organization and power relations they could bring about.

Vili Lehdonvirta, *The Blockchain Paradox: Why Distributed Ledger Technologies May Do Little to Transform the Economy*, POL'Y & INTERNET BLOG (Nov. 21, 2016), http://blogs.oii.ox.ac.uk/policy/the-blockchain-paradox-why-distributed-ledger-technologies-may-do-little-to-transform-the-economy.

Additionally, there might be economies of scope (with respect to rule making and rule enforcement) in providing the level of trust required to safeguard the operation of the trading system. *See, e.g.* Curry, *Global Perspectives* in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 77 ("Federated trust enables confidence and risk reduction."). This may be why, according to Lehdonvirta, systems such as RSCoin and R3 openly rely on trusted third parties. Lehdonvirta, *supra* ("R3's design seems to have something . . . which look[s] a lot like trusted third-party enforcers . . . . RSCoin likewise relies entirely on trusted third parties.").

[37] *Not-So-Clever Contracts*, ECONOMIST (July 28, 2016) [hereinafter *Not-So-Clever Contracts*], http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted ("[T]rusted parties, known as oracles, could supply the data to a blockchain[.]"); *The Curator*, THE DAO, https://daohub.org/curator.html [https://archive.is/jFmPb] ("A curator is a failsafe mechanism that indirectly prevents malicious actors from executing [a] 51% attack"); *see also What Is Ethereum Classic*, CRYPTOCOMPARE (Aug. 3, 2016, 11:05 AM), https://www.cryptocompare.com/coins/guides/what-is-ethereum-classic; *The DAO, the Hack, the Soft Fork and the Hard Fork*, CRYPTOCOMPARE (Sept. 28, 2017, 5:10 PM), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork.

[38] *Not-So-Clever Contracts*, *supra* note 37.

[39] In the DAO case analyzed next in Section III.A, the six "curators" were private individuals who, among other functions, pre-selected proposals. *The DAO, the Hack, the Soft Fork and the Hard Fork*, *supra* note 37. The DAO claimed:

> A Curator is a failsafe mechanism that indirectly prevents malicious actors from executing 51% attack. Curators do not add centralization to the DAO: they are nominated by the DAO Token Holders themselves, and can be fired at any time, for any reason. Curators curate the whitelist, the list of Contractors authorized to receive ether from the DAO.

development of applications and, in particular, smart contracts will increasingly rely on modules created and vetted by specialists: the supply side of the industry will likely be based on a chain of multiple vertically-linked suppliers.[40]

A. THE PRESENCE OF CENTRAL ENFORCERS

More revealingly, smart contracts may even require enforcers in a more traditional sense for contract completion.[41]

The Curator, *supra* note 37. Curators within the DAO only performed two functions:

> Check that the published Contract on the Ethereum blockchain matches the source code the Contractor claims to have deployed (this is done by comparing bytecode).
>
> Confirm that a Proposal comes from an identified person or organization. This is done by asking the entity submitting the Proposal to send a signed transaction with a certain set of data only known to the Curator and the author of the Proposal, thereby confirming the author of the Proposal.

Id. These two functions were also performed by token holders, who were also responsible for evaluating proposals, auditing proposals' "smart contract code," providing legal advice regarding proposals, and taking "economic responsibility" for the proposals. *Id.* However, their enforcement role became evident during evolution of the venture. Ryan Shea, *Simple Contracts Are Better Contracts: What We Can Learn from the Meltdown of the DAO*, BLOCKSTACK BLOG (June 17, 2016), https://blog.blockstack.org/simple-contracts-are-better-contracts-what-we-can-learn-from-the-dao-6293214bad3a#.ym078tjga ("The Ethereum community found itself in a position where it had to step in and reverse the damage, thereby essentially making a small number of players the enforcers of the truth of all contracts.").

[40] *See, e.g.*, Demian Brener, *The Ugly Truth About Blockchain*, MEDIUM (Sep. 29, 2016), https://blog.zeppelin.solutions/the-ugly-truth-about-blockchain-applications-73e55cad9582 (providing an example of such a module).

[41] Competitive arbitration implemented through "2-out-of-3 multisignature transactions" is one form of relatively conventional third-party enforcement. *See, e.g.*, NARAYANAN ET AL., *supra* note 14, at 278–79. Even Bitcoin works with a substantial degree of human rulemaking:

> [T]he initial version of the software was published by Satoshi Nakamoto (a pseudonym). In 2010, Nakamoto handed control of the project to Gavin Andresen, an Australian-born programmer living in the United States. Like any software, Bitcoin needs to be regularly updated to address bugs, security issues, and changes in the operating environment. Such an update can in principle change any aspect of the software, including accounting and ownership rules. Who gets to write the software and how that process is governed is therefore critically important to all participants in a distributed ledger system.
>
> In the case of Bitcoin, the software is governed by an ad hoc process involving a handful of informal institutions and power holders. . . . The software is open source and anyone can suggest changes to it, but technical authority to admit changes to the official version of the software is held by a team of five core developers

This presence of third party enforcement was clearly pointed out by "The DAO" incident occurring in 2016 in the Ethereum platform, which was then considered the paradigm of smart contracts,[42] and aimed to implement the "code is law" principle coined by Lessig,[43] according to which the code itself provides conclusive enforcement.[44] After an initial successful launch of

> appointed by Andresen. The core developers' power is constrained by an informal self-imposed charter, which states that significant changes to the rules require broad consensus from the community. . . . This governance process worked well when the changes to the code were uncontroversial bug fixes, but it has started to show signs of breaking down recently, because some decisions require choosing which stakeholders' interests to prioritise over others'.

Vili Lehdonvirta & Ali Robleh, *Governance and Regulation: Two Types of Rule-Making*, in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 43.

[42] *See, e.g.*, Kiviat, *supra* note 9, n.238 (citing Ethereum as a foundational smart contract blockchain application); Reyes, *supra* note 14, at 191 n.1, 201 n.61 (same). For additional information regarding Ethereum, see Ethereum, *White Paper: A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper (last visited Aug. 1, 2016) (Ethereum's foundational manifest); Ethereum, *Ethereum Homestead Documentation*, ETHEREUM HOMESTEAD, http://www.ethdocs.org/en/latest (last visited Aug. 1, 2016).

[43] LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006). A narrower version of the same concept is that of *Lex Cryptographia*: "blockchain technology raises a series of novel legal questions that refer to a new body of law—which we term *Lex Cryptographia*—or rules administered through self-executing smart contracts and decentralized (autonomous) organizations." Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SOC. SCI. RES. NETWORK 4 (Mar. 10, 2015), http://www.ssrn.com/abstract=2580664.

[44] Ethereum sees itself as a platform for all sorts of automatically-enforced contracts without intermediaries:

> Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.
>
> These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, *all without a middle man or counterparty risk*.

ETHEREUM BLOCKCHAIN APP PLATFORM, (emphasis added) https://www.ethereum.org/ (last visited Aug. 2, 2016). Ethereum also encourages users to:

> [C]reate a tradeable digital token that can be used as a currency, a representation of an asset, a virtual share, a proof of membership or anything at all. These tokens use a standard coin API, so your contract

The DAO, an incident showed that implementing this principle is harder than it seems, as a failure in the original drafting of the contract led to its subsequent revision, showing that its terms were not conclusive and the blockchain was not immutable.

The DAO (the acronym stood for "Decentralized Autonomous Organization") was a sort of venture capital fund structured as a smart contract to which any investor could contribute "ether," the Ethereum's cryptocurrency, thus purchasing shares ("tokens") and voting rights, which they then used on the projects they decided to support.[45] In June 2016, after it had raised up to $250 million from thousands of backers, it emerged that someone had used a bug in its code to "siphon" from its original owners about $60 million worth of ether.[46] After using similar tactics to fight a so-called DAO war for weeks,[47] the Ethereum team decided to implement a "hard fork." (A hard

> will be automatically compatible with any wallet, other contract or exchange also using this standard.

Id.

[45] *The DAO, the Hack, the Soft Fork and the Hard Fork*, *supra* note 37.

[46] Paul Vigna, *Ethereum Gets Its Hard Fork and the 'Truth' Gets Tested*, WALL ST. J. (July 20, 2016), http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested. The heart of the debate was how to characterize the action by the "hacker": while many observers considered it as theft, the hacker alleged that it was simply the pre-established reward for having detected a loophole in the code. In an open letter addressed to the DAO and the Ethereum community, this self-described "Attacker" argued the following:

> I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. *It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs*." I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO.

An Open Letter: To the DAO and the Ethereum Community, PASTEBIN, (June 18, 2016) (emphasis added), http://pastebin.com/CcGUBgDG. Apparently, "this withdrawal of funds, while unexpected, did not violate either Ethereum's or The DAO's rules, naïve as they may have been. Nor does it appear to have violated any laws." Patrick Murck, *Who Controls the Blockchain?*, HARV. BUS. REV. (Apr. 19, 2017), https://hbr.org/2017/04/who-controls-the-blockchain.

[47] *See* Mathew Leising, *The Ether Thief*, BLOOMBERG MKT. (June 13, 2017), https://www.bloomberg.com/features/2017-the-ether-thief/.

fork consists of modifying the software so that it will validate blocks that the previous version considered invalid. It can pursue different goals, from eliminating security hazards in the code to implementing new functions or, as in this case, reversing transactions.)[48] If the changes proposed by the Ethereum team were adopted by the community of users, by simply upgrading the software, this would effectively delete the allegedly fraudulent transactions and refund the money to its previous owners, but would endanger the conclusiveness of the contracting process. Consequently, "the Ethereum community found itself in a position where it had to step in and reverse the damage, thereby essentially making a small number of players the enforcers of the truth of all contracts."[49]

The hard fork therefore denied the conclusiveness or immutability that was predicated of smart contracts, which were supposed to have the law enshrined in the code, making enforcement and dispute resolution unnecessary.[50] In particular, the Ethereum team was accused of conflict of interests and, in particular, of supporting the conclusiveness of transactions only "until something goes wrong that impacts the interests of a centralized authority."[51] Some degree of centralization was made visible by the promoters' power to manage the system. Moreover, their ability to do so hinted that the possibility of similar interventions was present in all other blockchain applications.

[48] NARAYANAN ET AL., *supra* note 14, at 73. On the contrary, in a so-called soft fork, "all new blocks continue to meet the requirements of the old rules, so the old clients will accept new blocks as valid additions to the block chain. . . . Any change in the rules governing what constitutes the authoritative block chain will necessarily be a hard fork." Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 382 n.128 (2016).

[49] Shea, *Simple Contracts Are Better Contracts*, *supra* note 39.

[50] *Id.* ("There are two problems here. First, when Ethereum allows forks to happen and override smart contract code, it's giving up on 'code as law' and allowing the spirit of code to trump it when the execution deviates from the spirit. . . . Second, this casts doubt on the true decentralization of the system and invites regulators and oppressive regimes to step up in the future and apply pressure to reverse history and/or change the rules of the system. . . . Smart contracts are either 'code as law' or else they are mere social contracts."). The key issue is, in these terms, that the hard fork treated them as social contracts.

[51] Avtar Sehra*, Building a Decentralised Ecosystem*, SLIDESHARE, slide 9 (Aug. 18, 2016), https://www.slideshare.net/arcatomia/ethereum-classic-18-august-2016?qid=f687c929-6875-4c92-9f42-422ceaba64cc&v=&b=&from_search=7.

Consequently, the community was split and some important miners and exchanges started backing an alternative currency, called "Ethereum Classic" (ETC), which uses the original blockchain.[52] Those who held Ether on it retained their rights, but for the funds stolen in the DAO attack.[53] In the end, "that group of miners continued to mine the original (pre-fork) chain, essentially creating a new coin dubbed Ethereum Classic. By continuing on the non-forked chain, they . . . created two worlds: one where the DAO, along with all the consequences of its hack, still existed, and one where it never happened."[54]

This dual reality is possible because, while the only right that users of a conventional centralized currency have is to stop using it,[55] users of a cryptocurrency have another option: they can also fork the rules, meaning that they "would rather operate under a different rule set, and . . . go in a different direction from the lead developers."[56] This is visible in a hypothetical example, taking Bitcoin as a reference:

> We can think of the currency we had up until the fork as being Bitcoin [i.e., in the real case, Ethereum]—the big happy Bitcoin that everyone agreed on. After the fork it's as if, A-coin [i.e., Ethereum] corresponding rule set A and B-coin [i.e., Ethereum Classic] corresponding to rule set B. At the moment of the fork, everyone who owned one bitcoin receives one A-coin and one B-coin. From that point on, A-coin and B-coin operate as separate currencies, and they might operate independently. The two groups might continue to evolve their rules in different ways.
>
> We should emphasize that not just the software, or the rules, or the software implementing the rules forked—the currency itself forked. This is an interesting event that can happen in a cryptocurrency that couldn't happen in a traditional currency, where the option of forking is not available to users.[57]

[52] *See The DAO, the Hack, the Soft Fork and the Hard Fork*, *supra* note 37; Duncan Riley, *Ethereum Classic Takes Off Following Ethereum Hard Fork*, SILICON ANGLE (July 25, 2016), http://siliconangle.com/blog/2016/07/25/ethereum-classic-takes-off-following-ethereum-hard-fork/.

[53] Ian DeMartino, *As Ethereum Classic Forks, DAO Hacker Moves Funds*, INSIDE BITCOINS (Oct. 25, 2016, 12:05 PM), http://insidebitcoins.com/news/ethereum-classic-forks-dao-hacker-moves-funds/36505.

[54] *Id.*

[55] In general, most holders of claims in Williamsonian "relational contracts" (*see infra* note 80 and related text) are in a similar position: for instance, after failing in a shareholders' meeting to advance their proposals and change the course of the corporation, minority shareholders can only vote with their feet by selling their stock.

[56] NARAYANAN ET AL., *supra* note 14, at 171.

[57] *Id.* at 172.

The evolution of both coins in the market (here composed not only of investors but also of exchanges and miners), in terms mainly of price and volume, hints how adequate the two sets of rules are. For instance, Ethereum Classic immediately became the third most traded cryptocurrency behind Bitcoin and the hard fork version of ether.[58] Some months later, it had "refused to die despite the Ethereum Foundation's repeated attempts to kill it"[59] and looked relatively strong,[60] a remarkable achievement considering that it had suffered numerous attacks.[61] The survival of the two coins plus the fact that their total value was soon greater than the pre-forked value also suggest that the diversity of rules (with immutability in Ethereum Classic but more efficient breach in Ethereum)[62] and, perhaps, the availability of such a competitive process for setting rules are valuable, probably providing better adaptation, as well as better control of developers.

However, even if the goal of Ethereum Classic was to preserve the immutability of the blockchain and the conclusiveness of transactions, its claims of code-as-law were somehow diluted, by recognizing that "the infrastructure is not there to enforce and uphold law, it's only a protocol that allows execution of immutable transactions and programs."[63] Despite

[58] Riley, *Ethereum Classic Takes Off Following Ethereum Hard Fork*, *supra* note 52.

[59] Frances Coppola, *Ethereum's Latest Hard Fork Shows It Has a Very Long Way to Go*, FORBES (Nov. 26, 2016), https://www.forbes.com/sites/francescoppola/2016/11/26/ethereums-latest-hard-fork-shows-it-has-a-very-long-way-to-go/#6e4220f1443a.

[60] For example, on October 17th, 2016, the market capitalization of Ethereum Classic was 9.33% that of Ethereum, making it the fifth cryptocurrency according to this metric. Thirteen months later (November 10, 2017), however, its market capitalization had fallen to 4.83% of Ethereum and it was only the tenth cryptocurrency; and, even if its price had increased between those two dates by a multiple close to twelve, this was much less than Ethereum's 23.6 (numbers calculated by the author with data obtained from https://coinmarketcap.com/). Given that, at that point, the main difference between the two coins was the original conflict, the market (and, crucially, the exchanges, as Classic was only traded by a few of them) was apparently not very appreciative of the conservativeness of Ethereum Classic with respect to immutability.

[61] *See* Jamie Redman, *A Victorious Rebellion? Microsoft Investigates Ethereum Classic's Potential*, BITCOIN.COM (Sept. 27, 2016), https://news.bitcoin.com/microsoft-looks-rebel-ethereum-classic/.

[62] On efficient breach, *see supra* note 32.

[63] Sehra, *supra* note 51, at slide 10.

being presented as a decentralized, non-governed blockchain system, Ethereum Classic also relied on third-party enforcement, only in the more conventional form of state intervention.[64] As argued by one of its developers, the solution for failures should be based on "Legal Recourse. If anything goes wrong the infrastructure cannot be controlled into changing its state, recourse for financial crime and other illegal activities needs to take place through normal channels."[65] It can be concluded that, at least for fraud cases, Ethereum Classic relies on standard legal recourse (what could also be understood as a form of third-party contract completion) and blockchain integrity is dissociated from self-enforcement.[66]

Ethereum Classic was a paradigm, but it is not a unique case. Bitcoin itself suffered a similar experience in the summer of 2017, when trying to reach a consensus to solve the technical, economic, and ideological conflict between miners, who wanted bigger block sizes, and code developers, who stressed security.[67] There was substantial uncertainty, which initially harmed the coin price and seemingly also gave rise to the creation of another coin (named "Bitcoin Cash") through a hard fork.[68] The episode

[64] *Id.*

[65] *Id.*

[66] Moreover, only a few months after its inception, Ethereum Classic itself proposed a rather technical hard fork to deal with several attacks it was suffering due to vulnerabilities in its code. Understandably, and despite not changing the history of blockchain, the proposal posed risks and triggered a similar controversy, with some parties claiming it would breach the "dogmatic application of immutability" that had been the main reason to create this new cryptocurrency in the first place. Andrew Quentson, *Ethereum Classic Divided over the Proposed Hardfork*, CRYPTOCOINS NEWS (Oct. 14, 2016), https://www.cryptocoinsnews.com/ethereum-classic-divided-proposed-hardfork/.

[67] *See* Lulu Yilun Chen & Yuji Nakamura, *Bitcoin Is Having a Civil War Right as It Enters a Critical Month*, BLOOMBERG (July 10, 2017), https://www.bloomberg.com/news/articles/2017-07-10/bitcoin-risks-splintering-as-civil-war-enters-critical-month (stressing the opposite views of developers and miners).

[68] *Id.*; *see also* Frances Coppola, *The Fundamental Conflict at The Heart of Bitcoin*, FORBES (July 26, 2017), https://www.forbes.com/sites/francescoppola/2017/07/26/the-fundamental-conflict-at-the-heart-of-bitcoin/2/#7ecd3d15aac7 (stressing the traditional monetary conflict between value and liquidity); David Z. Morris, *Bitcoin's King Solomon Moment*, SLATE (June 6, 2017), http://www.slate.com/articles/technology/future_tense/2017/06/internal_conflict_could_split_bitcoin_in_half.html (stressing consequences for the different participants, including blockchain applications with different business models). *Contra* Samson Mow, *The Bitcoin Cash Fork Was a Dangerous Trick*, FORTUNE (Aug. 7, 2017), http://fortune.com/2017/08/07/bitcoin-cash-bch-hard-fork-blockchain-usd-coinbase/; Jake Smith, *The Bitcoin Cash Hard Fork Will Show Us Which*

showed again how the deficit in formal governance structures was decided by a hard fork, disciplining developers in the same way as the DAO incident suffered by Ethereum one year earlier.[69] The Bitcoin Cash event suggests that hard forks may become a structural and recurrent feature of these systems, somehow similar to hostile tender offers in the market for

Coin Is Best, FORTUNE (Aug. 11, 2017), http://fortune.com/2017/08/11/bitcoin-cash-hard-fork-price-date-why/ (defending the idea that "the split achieved the desirable outcome of allowing both visions of Bitcoin to compete in the free market."). At the time of writing, Smith's idea seemed to be winning the argument: the price of both coins combined was greater, and, even though Bitcoin prices had soared, Bitcoin Cash was the fourth cryptocurrency by market capitalization, equal to 7.48% of that of Bitcoin, and its price was 7.49% of that of Bitcoin (calculated on August 13, 2017 by the author with data obtained from https://coinmarketcap.com/; probably not fully informative given the relative lack of liquidity). Some days later, it had mined the first 8BM block but there were still some concerns about excessive concentration of miners. Josiah Wilmoth, *The First 8MB Bitcoin Cash Block Was Just Mined*, CRYPTOCOINS NEWS (Aug. 17, 2017), https://www.cryptocoinsnews.com/first-8mb-bitcoin-cash-block-just-mined/. The availability of the new coin did not satisfy all parties and yet another hard fork was expected to take place in November 2017. Anupam Varshney, *Bitcoin Is Splitting Once Again—Are You Ready?*, THE COIN TELEGRAPH (Aug. 18, 2017), https://cointelegraph.com/news/bitcoin-is-splitting-once-again-are-you-ready. However, the new coin was cancelled on November 8th. Mike Belshe, *Segwit2x Final Steps*, LINUX FOUND. (Nov. 8, 2017), https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html. In the following days, the price of Bitcoin fell while that of Bitcoin Cash soared, doubling its relative price to reach a maximum of 15.85% on November 10th (relying on prices given by https://coinmarketcap.com/currencies).

[69] Even if there have been few hard forks, the ones that have taken place illustrate that they may end up with different outcomes. In 2014, the MintPal exchange suffered a hack that led to two million USD in VeriCoin tokens being stolen. Subsequently, developers reclaimed the funds by what is said to be the first hard fork. Clay Michael Gillespie, *VeriCoin Developer Speaks with CCN on MintPal Hardfork*, CRYPTOCOIN NEWS (July 15, 2014), https://www.cryptocoinsnews.com/vericoin-developer-speaks-ccn-mintpal-hardfork/. Also in 2014, after Nxt had suffered a 1.75 million USD theft, developers also proposed a hard fork, but it was rejected. Most of the funds were recovered through negotiations but only after paying ransom to the hacker. Brandon Hurst, *$1.75 Million Hack Raises Prospect of Hard Fork: A Price Not Worth Paying* (Oct. 31, 2014), https://bitcoinblog.de/2014/10/31/1-75-million-hack-raises-prospect-of-hard-fork-a-price-not-worth-paying/. It has been alleged that the different outcomes were aligned with the different causes of the hacking and, consequently, the merits of the cases. Clay Michael Gillespie, *VeriCoin Developer: "The NXT Chain Should Not Be Rolled Back"*, CRYPTOCOIN NEWS (Aug. 15, 2014), https://www.cryptocoinsnews.com/vericoin-developer-believe-nxt-chain-rolled-back/. Bitcoin itself forked in 2010 after someone minted billions of bitcoins but, given that the network was still small, it was easily handled without much difficulty. *Id.*

takeovers or corporate control. Note that takeovers also often end up redirecting and splitting the assets involved, so that the takeover market also provides a discrete, competitive, market-led solution, alternative to the institutional, continuous, and evolutionary decision-making provided by formal corporate governance through, for example, corporate boards, proxy fights and general shareholders' meetings.[70] (On the contrary, hard forks launched to reverse an allegedly fraudulent transaction may, at least sometimes, be closer to a bank bailout, especially if developers, miners, and investors have close ties or are even the same persons, so that they all share a vested interest in reversing the transaction.)[71]

[70] One may interpret from this governance perspective the concerns. *See, e.g.*, Kathleen Breitman, *Why Ethereum's Hard Fork Will Cause Problems in the Coming Year*, BITCOIN MAGAZINE (Feb. 3, 2017), https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/ (stating, in essence, "hard forks are not effective for evolutionary change"). However, no doubt hard forks act as a disciplinary device for lead developers:

> In a sense, the lead developers are leading the parade. They're out in front, marching, and the parade will generally follow them when they turn a corner. But if they try to lead the march down a disastrous route, then the parade members might decide to go in a different direction. The lead developers can urge the community on, but they don't have formal power to force people to follow them if they take the system in a technical direction that the community doesn't like.

NARAYANAN ET AL., *supra* note 14, at 171. How effective they may be in this disciplinary task remains an open question. Most likely, as many market-driven processes, competition among participants will be a major determinant of overall efficiency. Similarly, as in the takeover market, collisions between efficiency objectives and distributional concerns are bound to arise: positive size-of-the-pie effects may well coexist with exploitation of the least-informed participants. *C.f., e.g.*, Gregg Jarrell & Michael Bradley, *The Economic Effects of Federal and State Regulations of Cash Tender Offers*, 23 J.L. & ECON. 371, 373 (1980). Similarly, the distribution of value gains may affect the incentives to launch hard-fork initiatives, in a similar manner to the effect that takeover rules, e.g., sharing takeover premiums, have been claimed to exert on the likelihood of takeovers. *Id.*

[71] *See* Frances Coppola, *A Painful Lesson for the Ethereum Community*, FORBES (July 21, 2016, 1:54 PM), https://www.forbes.com/sites/francescoppola/2016/07/21/a-painful-lesson-for-the-ethereum-community/#1b2f26cabb24 ("[T]he Ethereum central bank has directly recapitalized the DAO commercial bank by monetizing its debts."). The whole series of incidents also suggests that Bitcoin may in fact be more "regulated" or at least "governed" than is sometimes claimed. *Contra*, Gur Huberman, Jacob D. Leshno & Ciamac Moallemi, *Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System*, BANK FIN. RES. DISCUSSION PAPERS 36 (Sept. 5, 2017), https://helda.helsinki.fi/bof/bitstream/handle/123456789/14912/BoF_DP_1727.pdf. To understand its governance, one needs at least to consider the role played by code developers and allegedly concentrated miners.

B. Contract Completion in Smart Contracts

These cases teach some important general lessons. Furthermore, being controversial, they show the tensions and tradeoffs that the technology involves, which may be more informative than the usual summary of business models so common in the literature.

First, the tensions observed resemble the traditional conflict between the blind and automatic application of formal legal principles that should enable impersonal transactions and their nuanced qualification through exceptions based on principles of equity, good faith, or notice, which introduce a personal and often even political element and, as a consequence, are more suitable for personal exchange.[72]

Second, as in other attempts to enable impersonal exchange, it makes sense to argue for contract simplicity. For instance, the root of the DAO problem was that smart contracts face a tradeoff between security and complexity,[73] and the uncertain and changing environment emphasizes the need for adaptation. Furthermore, errors in computer code are prevalent and

[72] This conflict is visible in this summary of the pros and cons involved in the DAO incident:

> Users that did not support the hard fork point out that: code is law—the original statement of The DAO terms and conditions should stand under any circumstances; things that happen on the blockchain are immutable and they should never change regardless of what the outcome is; there is a slippery slope and once you modify/censor for one course/reason there is not a lot to keep you from doing it for other contracts; the decision to return the money is short sighted and you might reduce the value of ETH down the line based on your decision to act now; [and], this is a bailout. Users that supported the hard fork argued the code is law is too drastic of a statement at the current time and humans should have the final say through social consensus; the Hacker could not be allowed to profit from the exploit as it is ethically wrong and the community should intervene; the slippery slope argument is not valid as the community is not beholden to past decisions, people can act rationally and fairly in each situation; it would be problematic to leave such a big piece of the Ether supply in the hands of a malicious actor and it might harm the value of Ether down the line; this is not a bailout as you are not taking money from the community, it is just a return of funds to the original investors; it would stop an ongoing war between the white-hat hackers and the hacker that would demoralize the community; the exploit was big enough to take action and reverse it; [and], if the community acts now it will make people that are unethical think twice before they use Ethereum as their platform of choice.

What is Ethereum Classic, *supra* note 37 (punctuation modified by the author).

[73] *See* Shea, *supra* note 39.

impossible to eradicate, and they increase with complexity,[74] as with conventional contracts. Moreover, once a smart contract is implemented, it is not under the control of its creator, unless the power to change the code is allocated to a "master," with obvious centralization.[75] Automatic contracts therefore need to use simple computer code (some platforms meet this demand for simplicity by running most of the logic off the chain and having it upgraded by the majority of the parties[76]). A related point is made by Abramowicz in terms of the judgment that may be needed to "complete" contracts: "until computer programs can exhibit general artificial intelligence, they will lack judgment. They will not, for example, be able to determine whether vague contract provisions have been satisfied. Cryptocurrencies cannot solve the problem of incomplete contracts, and as long as contracts are incomplete, humans will need to resolve ambiguities."[77]

The role of simplicity and the scope for ex ante completion help to explain why blockchain seems to be gaining more ground

[74] See Joshua Bloch, *Extra, Extra—Read All About It: Nearly All Binary Searches and Mergesorts are Broken*, GOOGLE RES. BLOG (June 2, 2006), https://research.googleblog.com/2006/06/extra-extra-read-all-about-it-nearly.html, for an interesting example. It is said that "[o]n average, software comes with between 15 and 50 defects per 1,000 lines of code." *Not-So-Clever Contracts*, *supra* note 37.

[75] *See* Shea, *supra* note 39 ("[O]nce a smart contract is implemented, it takes on a life of its own and the code cannot be changed unless it is created with a 'master' or set of masters who can change the code.").

[76] For instance, in the case of Blockstack, by (1) "[encoding] minimal logic on the blockchain," which would "[o]nly define the parties involved in the agreement and allow them to jointly hold assets and authorize transfers"; (2) "[creating] a code agreement that all parties run *off of the chain*," with communication channels where parties can sign distribute, vote and upgrade the code agreement; and, (3) "have the parties run code off of the chain . . . [and] submit transfer requests" which go through when accepted by a majority of parties running the code. Shea, *supra* note 39 (emphasis added). For further development of the proposal, see Muneeb Ali & Ryan Shea, *A Token Mechanism for Growing the Blockstack Ecosystem of Decentralized Applications*, BLOCKSTACK TOKEN (Oct. 26, 2017), https://blockstack.com/tokenpaper.pdf.

[77] Abramowicz, *supra* note 48, at 362 (citation omitted). On this basis, Abramowicz argues that bitcoin is not really a system of peer-to-peer governance. First, given its limited scope of decisions and, in particular, the fact that such decisions involve no judgment: "It is an institution, however, that can resolve only one type of decision: whether purported transfers of Bitcoins will be validated and added to a list of approved transfers, known as the *block chain*." *Id.* at 361. Moreover, "[it] is coordinated in the same centralized manner as other open source projects." *Id.* at 367.

in the financial world and, in particular, in such areas as payments and even derivatives trading,[78] which are already quite standardized and in fact deal with legal commodities. Obviously, contractual and property simplicity are negatively correlated to the value of transactions: for low-value transactions, complex contracts are too costly to write and enforce, and low-value assets are not valuable enough to define multiple rights on them. Understandably, blockchain and smart contracts also develop more easily in low-value contexts.[79]

Lastly, blockchain clearly adds value by providing verifiability on the *content* of contractual documents. However, it is less clear to what extent or in which cases it is able to make contractual *performance* verifiable by third parties or even make verification unnecessary, except for very abstract and extremely formalized contracts. Therefore, consequences of blockchains on relational contracts are likely to be small, if by "relational" we mean contracts that are completed by the parties ex post, sometime in the future after they committed to the contract.[80] The contract was left incomplete because it would have been inefficient or even impossible to complete it. Verifiability of the contractual content (where blockchain probably enjoys its stronger comparative advantage) seems just a tiny element to substantially affect these tradeoffs.

On the other hand, blockchains could seemingly have a greater effect on the functioning of relational contracts, when by "relational" we mean an exchange safeguarded by reputation or the expectation of future trade gains, in a way the opposite of impersonal exchange.[81]

[78] *See*, *e.g.*, INT'L SWAPS AND DERIVATIVES ASS'N (ISDA), THE FUTURE OF DERIVATIVES PROCESSING AND MARKET INFRASTRUCTURE 23 (2016), https://www2.isda.org/attachment/ODcwMA==/Infrastructure%20white%20paper.pdf (arguing that blockchain holds great potential in the derivatives industry and advising to develop mechanisms to designate blockchain records as final as early in the transaction lifecycle as possible).

[79] ALLENS LINKLATERS, *supra* note 30, at 14–15.

[80] *C.f.* OLIVER E. WILLIAMSON, THE ECONOMIC INSTITUTIONS OF CAPITALISM: FIRMS, MARKETS, RELATIONAL CONTRACTING (1985). In a sense, Shea's proposed code agreement would place the relational element outside the blockchain. Ali & Shea, *supra* note 76.

[81] *C.f.* Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615, 616 (1981) ("[E]conomists . . . have long considered 'reputations' and brand names to be private devices which provide incentives and assure contract performance in the absence of any third-party enforcer"); Carl Shapiro, *Premiums for High*

In this context, we must distinguish two types of blockchain applications:

First, applications enabling business-business (B2B) transactions could rely on "private" or "permissioned" systems, which are open only to preapproved users and in which the consensus may be driven by a previously established set of nodes.[82] In this vein, private blockchains should expand rapidly in supply chain management, revamping the existing and mostly closely-knit networks of suppliers, manufacturers, and distributors, which are already characterized by phenomena such as "contract manufacturing,"[83] as well as "virtual integration."[84] Financial institutions are pioneers in this regard.[85] However, from the perspective of blockchain, these

Quality Products as Returns to Reputations, 98 Q.J. ECON. 659, 659–60 (1983) ("[R]eputation formation is a type of signaling activity . . . the faithful strategy involves foregoing the opportunity to earn profits through quality reductions.").

[82] *See* Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (Aug. 7, 2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (describing the comparative advantages of public and private blockchains).

[83] Benito Arruñada & Xosé Henrique Vázquez, *When Your Contract Manufacturer Becomes Your Competitor*, HARV. BUS. REV. 135, Sept. 2006, https://hbr.org/2006/09/when-your-contract-manufacturer-becomes-your-competitor. *See also* IBM INST. FOR BUS. VALUE, FAST FORWARD: RETHINKING ENTERPRISES, ECOSYSTEMS AND ECONOMIES WITH BLOCKCHAINS (2016), https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03757USEN (describing the effects of blockchain on organizational structure).

[84] Benito Arruñada, *The Quasi-Judicial Role of Large Retailers: An Efficiency Hypothesis of Their Relation with Suppliers*, *in* THE ECONOMICS OF CONTRACTS: THEORIES AND APPLICATIONS 337 (Eric Brousseau & Jean-Michel Glachant eds., 2002). A prominent example is that of Wal-Mart. *See, e.g.*, Kim S. Nash, *Wal-Mart Turns to Blockchain for Tracking Pork in China*, WALL ST. J. (Oct. 19, 2016, 4:43 PM), http://blogs.wsj.com/cio/2016/10/19/wal-mart-turns-to-blockchain-for-tracking-pork-in-china/.

[85] According to the CEO of IBM, "Financial institutions are becoming early adopters: The World Economic Forum estimates that 80% of banks are working on blockchain projects." Ginni Rometty, *How Blockchain Will Change Your Life: The Technology's Potential Goes Way Beyond Finance*, WALL ST. J. (Nov. 7, 2016, 7:25 PM), http://www.wsj.com/articles/how-blockchain-will-change-your-life-1478564751. "Having initially been sceptical [sic] about [blockchain technology] because of worries over fraud, banks are now exploring how they can exploit the technology to speed up back-office settlement systems and free billions in capital tied up supporting trades on global markets." Martin Arnold, *Big Banks Plan to Coin New Digital Currency: Group of Major Lenders Seeks Industry Standard for Settlements*, FIN. TIMES (Aug. 23, 2016), https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c. However, there are more general initiatives such as MultiChain, which "helps organizations to build and deploy blockchain applications with speed," use managed

systems will face a basic contradiction: the smaller the network, the smaller the extent and the fewer the advantages of decentralization, and the easier it may be to manipulate it.[86] They may therefore end up with little decentralization, little disruption, and even some risk of collusion among incumbents. The advantage of blockchain in making the *content* of contracts (as opposed to contractual *performance*) verifiable might make it unsuitable for contracts which, on purpose, are not formalized in order to ensure self-enforcement.[87]

Second, the comparative advantage of blockchain applications would be considerably enhanced if the technology fulfills its promise of enabling individual users to own and keep full control of their historical record of transactional data, which is now in the hands of third-party centralized data silos (such as Google, Facebook or Booking). Availability and ownership of transactional data would make it possible for individuals to, first, accumulate reputational capital; and, then, deploy such capital to safeguard their transactions across multiple markets and relying on different applications. The system could benefit from massive economies of scale and scope, and could achieve secure personal transactions with anonymous parties, therefore providing an effective alternative to impersonal (i.e., meaning asset-based) exchange. Difficulties are numerous, however. For

permissions, which allows organizations to "[d]ynamically control who can connect, send and receive transactions, create assets, streams and blocks." MULTICHAIN: OPEN SOURCE PRIVATE BLOCKCHAIN PLATFORM, http://www.multichain.com/ (last visited Oct. 6, 2017). The chain is therefore "as open or as closed as you need." *Id.* The big question on private blockchain: What is its comparative advantage with respect to existing systems for data management? A preliminary answer rests on the additional capabilities provided by its peer-to-peer distributed structure, which should at least reduce the risks inherent in centralized control present even in vertically integrated structures due to agency problems.

[86] *See, e.g.*, NARAYANAN ET AL., *supra* note 14, at 34–38 (explaining a type of blockchain manipulation and confirming the role of honest nodes in preventing the success of a manipulation attempt).

[87] *See generally* Gillian K. Hadfield & Iva Bozovic, *Scaffolding: Using Formal Contracts to Support Informal Relations in Support of Innovation*, 5 WIS. L. REV. 981, 1019–32 (2016) (listing eighty-nine quotations from various companies regarding their approach to certain aspects of agreements and contracting). In Europe, this seems to affect even large recurrent transactions. For instance, it has been common practice for some big retailers and their main suppliers of consumer goods to write, but not sign, detailed and long contracts to organize their continuous relationships—allegedly to impede judicial interference (according to private conversations with practitioners).

instance, reaching such economies without some type of centralization, and—what may be the same—making the necessary investments without any possibility of capturing value in the future.

IV. BLOCKCHAIN AND PROPERTY, IN REM, RIGHTS

A. THE NEED FOR INTERFACES BETWEEN PERSONAL AND REAL RIGHTS

One of the key attributes of a public ledger currency platform is "a protocol for sending, receiving, and recording value securely using cryptographic methods . . . ."[88] A key question is to what extent, in addition to exchanging value, these systems are capable of exchanging property in rem rights.[89] Exaggerated but conveniently imprecise claims are common—for instance, one of the authors of the Walport Report asserted that "[u]npermissioned ledgers can be used as a global record that cannot be edited: for declaring a last will and testament, for example, or *assigning property ownership*."[90]

In fact, however, even most of the pioneer agents doing simple transactions, such as trading in Bitcoin, rely at least on intermediaries such as exchanges (digital marketplaces)[91] and

[88] David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* 1 (Coase-Sandor Inst. for Law & Econ., Working Paper No. 685, 2014), http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2349&context=law_and_economics.

[89] *Compare* Merrill & Smith, *supra* note 3 (discussing various aspects and criticisms of the *numerus clausus* principle, which holds that property rights need to conform to a closed number of standardized forms), *with* Hansmann & Kraakman, *supra* note 3 (disagreeing with Merrill and Smith's analysis, discussing requirements for the establishment of property rights, and setting out conditions to be used in assessing the efficiency of alternative property rights regimes).

[90] Simon Taylor, *Definitions*, *in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 17 (emphasis added).

[91] To users, they perform the same functions as banks (accept deposits in exchange for a mere promise to return them later, make payments, exchange electronic and fiat currencies, transfer funds, match clients, etc.) but also suffer similar risks, including bank runs, Ponzi schemes, and hacks, which are the electronic equivalent of break-ins. NARAYANAN ET AL., *supra* note 14, at 88–94. Before 2013, exchanges had experienced a failure rate of forty-five percent according to a study. *Id.* at 90. They also act as organized markets, in a similar way to organized fiat currency exchanges, even if users can disintermediate them to trade directly with other users. *Id.* at 99.

wallets (digital storage services).[92] Even if such intermediaries have often been insecure,[93] suffering frequent fraudulent attacks,[94] their presence is not necessarily bad.[95] Even though, as blockchain partisans rightly point out, specialized enforcement and, in general, intermediation, entail agency costs, they enjoy the advantages of specialization.[96] Economic growth is based on efficiently trading off specialization advantages and agency costs.

In more complex blockchain applications, in which parties trade claims on assets existing outside the blockchain ledger,

[92] The importance of these interfaces can also be seen in the need for peer-to-peer organizations and, in particular, banks, to own real assets in order to develop a valuable reputation, and therefore to be recognized as a legal person:

> The obstacle [of cryptocurrency banks], however, is solely a legal one: a fully functional bank must be able to own real assets because a primary function of a bank is to invest funds. A peer-to-peer institution could own assets only if the legal system recognized the peer-to-peer institution as legitimately existing and having a form of personhood sufficient for the ownership of property. Real property purchased by a trust, for example, might be held in the name of the public key or in the name of the cryptocurrency as a whole.

Abramowicz, *supra* note 48, at 413.

[93] For Bitcoin, the blockchain itself has been resilient but the wallets and exchanges have not: "[U]sing hacker-proof bitcoin requires going through intermediaries such as exchanges to convert real-world currency into crypto-cash, and 'wallets' to store it. These have proved anything but secure, which arguably defeats the purpose of bitcoin's trust-free world." *Blockchain: The Next Big Thing*, THE ECONOMIST (May 9, 2015) [hereinafter *Blockchain: The Next Big Thing*], http://www.economist.com/news/special-report/21650295-or-it-next-big-thing. *See also* Jamie Redman, *The Bitcoin Exchange Thefts You May Have Forgotten*, BITCOIN NEWS (Feb. 3, 2017), https://news.bitcoin.com/bitcoin-exchange-thefts-forgotten/ (describing a subset of the approximately fifty most important exchange thefts up to January 2017).

[94] *See* Izabella Kaminska, *Bitcoin Bitfinex Exchange Hacked: The Unanswered Questions*, FIN. TIMES (Aug. 4, 2016), https://www.ft.com/content/1ea8baf8-5a11-11e6-8d05-4eaa66292c32 (discussing a recent bitcoin exchange hack, listing a set of recent and significant thefts from bitcoin exchanges, and mentioning frequency of high profile hacking incidents since 2009). This supports the argument by Evans: "Current claims that public ledger platforms can conduct financial transactions more efficiently ignore the inefficiencies associated with the incentive and governance systems and the likely costs associated with regulation of these platforms and complementary service providers such as vaults, wallets, and exchanges." Evans, *supra* note 88.

[95] An obvious example of the value of intermediaries is that, without a central administrator, blockchain systems are "unforgiving: there is no helpdesk to reset a lost password . . . ." *Blockchain: The Next Big Thing*, *supra* note 93.

[96] *See* Evans, *supra* note 88 (mentioning the costs associated with regulation and complementary services providers like exchanges).

these interfaces between the digital and the real worlds resemble the traditional interface between contractual (in personam) and property (in rem) rights.[97] With the exception of systems purely based on possession, contracting property requires at least one intermediary (a registry or a court) between the world of mere claims (i.e., in personam rights) and the real world of in rem rights.[98] For example, in land law, two contradictory chains of title deeds could survive for a long time, but (1) at any point in time at most one individual is holding possession of the claimed right on the specific real asset; (2) most importantly, for upgrading one of the claims in a right with in rem consequences, what is needed is a third-party enforcer representing the interests of all potential rightholders and not only the interests of those in the chain of title—a crucially important aspect for blockchain applications.[99] Note that, in a

[97] The Cuber initiative involving an Estonian bank provides an example of the in personam nature of the rights acquired by users with respect to the intermediaries:

> The bank [LHV] enters the color identities into the code of the cryptocurrency Bitcoin. LHV guarantees the asset value of the particular pieces of Bitcoin whomever owns them. In their case the pieces of cryptocurrency represent Euro. When someone performs a transaction in Euro in Cuber, the properties of the color-coded cryptocurrencies are transferred so that they represent a Euro value with a new owner. The value of the Bitcoin currency in this context is completely uninteresting. The cryptocurrency is used as a way to store information, and LHV determines what this information represents in terms of value. This is not very different from the activity of a bank. The bank is currently responsible for what the digital codes in their databases represent in terms of value, which they also reconcile with central banks, markets, and so forth.

KEMPE, *supra* note 24, at 19. *See also* CUBER, http://www.cuber.ee/en_US/ (last visited Oct. 17, 2016) (Cuber home page).

[98] *See, e.g.*, Benito Arruñada, *The Titling Role of Possession*, *in* LAW AND ECONOMICS OF POSSESSION 207, 211 (Yun-chien Chang ed., 2015) (discussing judges' possible adjudicatory approaches to a hypothetical property dispute involving both in rem and in personam rights). *See generally* LAW AND ECONOMICS OF POSSESSION (Yun-chien Chang ed., 2015) (presenting analyses of various aspects of possession).

[99] A pioneer developer of applications for land registries, Factom, put it this way:

> Bitcoin, land registries, and many other systems need to solve a fundamental problem: proving a negative. They prove some "thing" has been transferred to one person, and prove that thing hasn't been transferred to someone else. While proof of the negative is impossible in an unbounded system, it is quite possible in a bounded system. *Cryptocurrencies solve this problem by limiting the places where transactions can be found.* Bitcoin transactions can only be found in the Bitcoin blockchain. If a relevant transaction is not found in the

sense, a chain of paper title deeds is also "virtual," as it reflects mere claims;[100] therefore, if parties to the contract agree, it can support trade without necessarily having any real effect in terms of the traded assets that it purports to represent.

This account is consistent with analyses of blockchain applications in "smart property" that use examples in which they are in fact describing transfers of possession instead of transfers of ownership—for instance, the running example of a "car whose *ownership* is controlled through a block chain" used in chapter eleven of Narayanan et al.,[101] immediately turns out to be a transfer of *possession*:

> The block chain transaction doesn't *merely* represent a change in ownership of the car: it *additionally* transfers actual physical control or possession of the car. When a car is transferred this way the earlier owner's key fob stops working and the new owner's key fob gains the ability to open the locks and start the engine. Equating ownership with possession in this way has profound implications.[102]

The implications are indeed profound but they are achieved by transforming ownership into possession—that is, by enforcing only a single right in the asset. The price being paid is huge: the modern economy is based on the specialization (or, some would say, separation) of ownership and control (that is, in its simplest sense, possession). If blockchain's smart property is limited to possessory rights, the word "merely" in the preceding quotation should be excised and the word "additionally" replaced by "only". In practical terms, this limits stand-alone (no trusted third parties) applications of smart property to low-value assets,

> blockchain, it is defined from the Bitcoin protocol perspective not to exist and thus the BTC hasn't been sent twice (double spent).

FACTOM, BUSINESS PROCESSES SECURED BY IMMUTABLE AUDIT TRAILS ON THE BLOCKCHAIN 5 (2014) (emphasis added), https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf?raw=true.

[100] The "chain" in "blockchain" comes about from the fact that each block is linked cryptographically to previous blocks. Jeremy Clark, *Foreword* to NARAYANAN ET AL., *supra* note 14, at XXI. This linkage resembles the links in the chain of title deeds used to provide evidence on property transactions, but in the case of title deeds there is a legal linkage between successive grantors and grantees. In a sense, it is closer to the physical indenture of medieval documents executed in two or more copies with edges correspondingly severed as a means of identification.

[101] NARAYANAN ET AL., *supra* note 14, at 272 (emphasis added).

[102] *Id.* at 274 (emphasis added).

as Narayanan et al. themselves seem to conclude a few pages later.[103]

In one respect, the decision system used by the blockchain *seems* closer to the one applied in property law to real property than to bank or cash money: blockchain decisions are based on gathering users' consents, and this may look similar to the transfer of ownership in real property, where the consent of rightholders is required to transfer in rem rights.[104] If *S* transfers to *B* a right held in rem by *O*, *S* may acquire an in personam claim against *B* but does not in any way affect *O*'s right. Similarly, transferring bitcoins requires a consensus of verifiers to validate the hashes. (In contrast, in a bank transfer it is only the banks involved who certify the transfer, while cash changes hands by merely transferring the possession of the bills. Cash transfers do not even leave a record: parties are constantly solving the "who owns what" question without relying on a formal "enforcement apparatus" except for the simple transfer of possession. Bitcoin is similar to cash in also being a bearer instrument,[105] but with records and an element of consent.)

Nevertheless, there are two fundamental differences between the systems for gathering consents in blockchain and property. First, blockchain users are more like observing spectators than rightholders; therefore, their incentives are not necessarily well aligned. Second, not all rightholders in the real assets are blockchain users; therefore, any purging procedure would require additional mechanisms to ensure that the interests of these rightholders are represented. In rem rights require all rightholders to grant their consent, not only those listed in a paper-based chain of title deeds or in the blockchain.

[103] However, they are led to that conclusion more for the need of third-party human judgment to complete transactions:

> The main advantage of smart property is the efficiency of ownership transfer, which can be done from anywhere at any time. For sales of items less valuable than a car (e.g., a smartphone or computer), disputes are unlikely to end up in court, and so nothing is lost in that regard. For such items, atomic transactions are a useful security feature.

Id. at 284.

[104] Benito Arruñada, *Property Enforcement as Organized Consent*, 19 J.L. ECON. & ORG. 401 (2003) [hereinafter Arruñada*, Property Enforcement*]; ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6.

[105] Andreessen, *supra* note 16.

These are serious concerns when it is claimed that "any type of asset can be transferred using the blockchain".[106] The legal effects of such transfers, at least, would be limited to the transferring parties.[107] Indeed, property rights are in the sphere of public ordering,[108] and pure "privacy" is only viable when parties trade in contractual claims.[109] As this has obvious welfare implications in terms of weaker enforcement,[110] parties understandably demand in rem rights. Meeting this demand requires the intervention of a third party with a necessarily public function, as it must be impartial to all and prevail over the parties to any given contract.[111] To start with, such a third party is necessary to define the set of legal rightholders and the mechanisms and evidentiary requirements for them to convey their consent with respect to intended transactions. It is revealing that blockchain initiatives often demand a more active role from governments in setting standards than in essence such a definition entails.[112]

These concerns are also echoed in the caveats often introduced when foreseeing blockchain applications. For example, a famous entrepreneur claimed that

> 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.[113]

Note, however, the "digital" adjective in the first sentence: one cannot send real property over the Internet or, more precisely, one cannot even transfer possession of real property over the Internet. A somehow similar caveat is introduced by Abramowicz when he considers the limitations of bitcoin:

> [W]hat makes Bitcoin remarkable is that it settles the most controversial issue—who owns wealth—without need for a law

[106] *The Great Chain of Being Sure About Things*, *supra* note 14, at 20.

[107] Abramowicz, *supra* note 48, at 365 ("Peer-to-peer law is most plausible as a mechanism of voluntary private ordering.").

[108] Arruñada, *Property as Sequential Exchange*, *supra* note 4.

[109] *Id.*; Arruñada, *Coase and the Departure from Property*, *supra* note 4.

[110] ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 18–24.

[111] Arruñada, *Coase and the Departure from Property*, *supra* note 4, at 305; Arruñada, *Property as Sequential Exchange*, *supra* note 4.

[112] *See supra* note 78 and accompanying text, on financial derivatives and *infra* Section IV.B, on the registration of legal organizations.

[113] Andreessen, *supra* note 16 (emphasis added).

> enforcement apparatus. Bitcoin can be seen not just as a currency, but more grandly as an institution that creates and enforces property rights. It is an institution, however, that *can resolve only one type of decision: whether purported transfers of Bitcoins will be validated and added to a list of approved transfers, known as the block chain.*[114]

Note that the implicit meaning of "property rights" in the previous quotation is that of contract, in personam, rights. For the same reason, it is understandable that enforcement of peer-to-peer decision systems is easier when they deal with digital resources being held in escrow. Not only the losing party is less effective in preventing enforcement but courts are unlikely to interfere because usually there are no claims by third parties.

B. OTHER INSIGHTS FROM THE THEORY OF PROPERTY RIGHTS

Additional aspects of blockchain can be enlightened by specific elements of the theory of property, in rem, rights. First is the distinction between initial and recurrent allocation of rights, which is a requirement for in rem rights.[115] Blockchain discussion and initiatives are still too incipient to have suffered from the general proclivity in conventional property titling and administrative simplification to overemphasize the initial allocation of property rights with little attention being paid to their recurrent allocation.[116] However, even in the implausible scenario that recurrent allocation could be produced in a safer manner within a blockchain-based technology, such a system would require at least two public interventions in order, first, to produce some sort of "first registration" (for property assets such as land and companies subject to public titling; less so for those others lacking it, such as diamonds); and, second, to define the blockchain as the only or at least a privileged source of judicial evidence for titling purposes.

[114] Abramowicz, *supra* note 48, at 361 (emphasis added).

[115] Benito Arruñada, *Property as an Economic Concept: Reconciling Legal and Economic Conceptions of Property Rights in a Coasean Framework*, 59 INT'L REV. ECON. 121 (2012). In particular,

> property, in rem, rights are only transacted in a two-step procedure which includes a first step corresponding to the conventional private contracting between the parties, with effects of an in personam nature; and a second, relatively "public," step which is capable of granting universal in rem effects because public authorities more or less explicitly represent the interests of all interested parties.

Arruñada, *Coase and the Departure from Property*, *supra* note 4, at 313.

[116] Arruñada, *Property as Sequential Exchange*, *supra* note 4.

In contrast, blockchain applications do follow the path of common efforts in property titling and administrative simplification in "paying scant attention to legal rights,"[117] despite this being the main determinant of enforceability and, therefore, economic value. This bias is highly visible in the diagnoses of traditional systems by blockchain entrepreneurs trying to apply the technology in the area of property titling, whose policy failures they narrowly attribute to poor data management; e.g., "[t]he failure of [traditional property registry software projects] to effect change can be traced to design flaws that ultimately leave them opaque to would be auditors while making the information they store overly pliable."[118] However, in reality, the main problem of property registries is not archiving information, but producing reliable information. That is, it is not a problem of *keeping* a record of perfectly "purged" property rights, but purging them and making sure that transactions are not contradictory with preexisting property rights and do not create new collisions of claims.[119] Despite the fact that this is mainly a legal issue, not a technological issue, blockchain applications in property registration focus instead on archiving and on keeping the integrity of the information, disregarding how the information is produced and, especially, the whole process of how property rights are purged of contradictions. Moreover, if this purging is something for which blockchain is perhaps of little use,[120] claims on the potential of the technology in this area should be substantially diluted.[121]

[117] *Id.* at 3; *see also id.* at 20–24.

[118] Dobhal Abhishek & Matthew Regan, Immutability & Auditability: The Critical Elements in Property Rights Registries 3 (2016) (paper prepared for presentation at the 2016 World Bank Conference on Land and Poverty).

[119] For example, saying that "many of the potential benefits of utilizing the blockchain [for 'land administration'] assume that a base layer of land information (titles, deeds, survey plans) exist and that the data is accurate" (Anand Aanchal, Matthew McKibbin, & Frank Pichel, Colored Coins: Bitcoin, Blockchain, and Land Administration 13 (2016) (draft of paper prepared for presentation at the 2016 World Bank Conference on Land and Poverty)) comes close to assuming perfect information and seems, for the reason given in the text, inadequate.

[120] As seemingly recognized when asserting that "[b]lockchain will not help to identify who has what right and to where. It will not resolve property rights disputes as properties are brought into the formal system. Most importantly it won't resolve the tedious and time consuming process of collecting, verifying and bringing data into the system." *Id.* at 3.

[121] This may help to explain why projects stall soon after big and seemingly exaggerated announcements; for example, Honduras. Pete Rizzo, *Blockchain*

A similar criticism is deserved by the Swedish inter-agency initiative to apply the blockchain to land conveyancing and registration, which considered that the main problems of the current Swedish Land Register were:

> that Lantmäteriet [Sweden's land registry] is only involved in a few steps at the end of the real estate transactions. As a consequence of this the majority of the process is not transparent, in other words, visible to the public or other stakeholders. . . . that the system is slow at registering real estate transactions. The time between the signing a legally binding purchasing con-tract [sic] and when Lantmäteriet receives the bill of sale and make the approval of the title is often three to six months. . . . [and] that the issues above have resulted in sellers, buyers, banks and real estate agents being forced to create their own complex, red tape, processes for agreements between them since they have to make sure that things can't go wrong, and because the value of the transactions is large.[122]

However, these three points in fact deserve serious qualifications.

First, it is not fully true that land registries are "involved in a few steps at the end of the real estate transactions"[123] because they provide crucial information on possible conflicting claims from the beginning and during the whole contracting path. For instance, in step three of the conventional conveyancing process described by Kempe, the Swedish real estate "agent contacts Lantmäteriet and orders an excerpt from the real estate registry database in order to check the information about the property, i.e. that the seller is in fact the owner and can sell the property."[124] Similar contacts are made in steps ten and twenty-one, before signing the purchasing contract and before the closing "to ensure that there aren't any problems that would prevent the sale of the property,"[125] and further contacts are made by banks in connection with mortgages at steps twenty-five and twenty-seven.[126] Moreover, there are costs and benefits

Land Title Project 'Stalls' in Honduras, COINDESK (Dec. 26, 2015, 3:31 PM), http://www.coindesk.com/debate-factom-land-title-honduras/. An anonymous commentator to Rizzo put this sharply in focus: "This is an example of some startup getting way ahead of themselves and declaring that just because they were talking to some government officials that made it 'a deal with the Honduras government'. It's like when startups have a bank account and then list the bank as their 'partner.'" *Id.*

[122] KEMPE, *supra* note 24, at 8–9.

[123] *Id.*

[124] *Id.* at 23.

[125] *Id.* at 24.

[126] *Id.* at 25.

associated with transparency. The tradeoff cannot always be assumed to be necessarily positive.

Second, the typical complaint that the systems are "slow at registering real estate transactions"[127] must be taken with a grain of salt, as most of the total time spent during the conveyancing of real estate is usually dedicated by parties to activities such as advertising, bargaining, surveying and inspecting properties, checking borrowers' creditworthiness, etc.,[128] activities that have little to do with the bureaucratic processes themselves. Consequently, two doubts emerge about, first, the time that is really spent in the bureaucratic steps that could therefore be shortened by the application of blockchain or other similar technologies; and, second, the economic value of such time savings. In other terms: for most transactions, shortening the time may have little value, especially when parties with an urgent need can effectively process the transaction in a much shorter time period.

Lastly, it is an empirical question how much security is in fact provided by alternative systems, blockchain included, especially at the beginning. New systems always need a learning period for their weaknesses to be revealed, while old systems offer the advantage of having accumulated such knowledge over millions of previous transactions.

V. ASSESSING BLOCKCHAIN APPLICATIONS IN PROPERTY

The previous analysis provides a basis for ascertaining the potential of blockchain technology and building predictions about the areas of contractual and property transactions that will be most hospitable for blockchain applications, their expected impact, and any circumstances that may hinder or enable their development.

I will now discuss the major issues in the area of property, broadly defined in order to cover the comparative advantage of different types of intermediaries and solutions, including the limitations and opportunities in the areas of property conveyancing and deed recordation, as well as company and property registration.

[127] *Id.* at 8.

[128] *See*, *e.g.*, *id.* at 23–25.

For a start, three cautionary notes are in order. First, remember the above-mentioned social element in property rights. Even Nick Szabo seems to be contemplating in personam rights when implementing his idea of property clubs: "Actually getting end users to respect the property rights agreed upon by this system will be dependent on the specific nature of the property, and is beyond the scope of the current inquiry."[129] Certainly, he immediately asserts that "[t]he purpose of the replicated database is simply to *securely agree on who owns what,*"[130] and this "securely agree" is essential to move from in personam to in rem.

Second, decentralization is limited in the real world because individuals tend to misbehave with respect to security:

> We were able to achieve decentralization only because we equated possession with ownership—owning a car [the asset being taken by the authors as a running example] is essentially equivalent to knowing the private key corresponding to a designated transaction on a block chain . . . . If we reduce ownership to the problem of securing private keys, it raises the stakes for digital security, which is a difficult problem with humans being a weak link. Programmers have endeavored to write bug-free code for decades, but the challenge remains elusive. Designers of cryptosystems have tried for decades to get non-technical users to utilize and manage private keys in a way that resists both theft and accidental loss of keys, also with little progress. If the model of decentralization relies excessively on private keys, cars might get stolen by malware or in phishing attacks, and the loss of a key might turn your car into a giant brick. While there could be fallback mechanisms to cover these types of events, inevitably such mechanisms tend to lead us back toward intermediaries and centralized systems, chipping away at the benefits of the decentralized model that we were striving for.[131]

This issue is present in all types of applications, but, understandably, it especially constrains those in which the stakes are higher, leading people to demand greater security.

Lastly, misbehavior with respect to security is only an instance of a broader and deeper phenomenon: individual freedom has a price in terms of individual responsibility that not all individuals are always willing to pay. Instead, knowing their own weaknesses, they often trust more and prefer to rely on

[129] Nick Szabo, *Secure Property Titles with Owner Authority*, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/securetitle.html (last visited Nov. 13, 2017).

[130] *Id.* (emphasis added).

[131] NARAYANAN ET AL., *supra* note 14, at 283.

centralized solutions based on private and public custodian agents.[132] This preference for third-party custodians imposes a particularly serious constraint on property applications because the universal nature of property requires that the same rules be applied to all rightholders. In a hypothetical, fully-decentralized property system, all individuals would therefore be granting or denying their consent to all sorts of intended transactions that might affect their property rights. Consequently, they would become the only custodians not only of their cryptographic keys (to receive notice and grant consent) but also of the legal integrity of their rights.

A. Conveyancing and Property Titling

The impact of the blockchain on conveyancing and property titling will be affected by the basic characteristics of both legal processes, which, in line with the incentives of participants, are mostly private in conveyancing and intrinsically public in registration.[133] In particular, they are defined by the fact that in all property systems parties are free to choose their lawyers, conveyers, and notaries public.[134] On the contrary, third-party protection leads the law to universally restrict their choice of the office that records their titles or the registrar that preserves and reviews their rights, as well as the judge who presides over a suit of quiet title or any equivalent judicial procedure.[135] Therefore, blockchain should find it easier to expand into notarization and data archiving,[136] but will find it more difficult to replace centralized land registries, especially in jurisdictions such as Australia, England, Germany and Spain that have registries of

[132] Note that this option makes considerably more sense under realistic behavioral assumptions, while the game-theory analyses applied to developing blockchains often assume perfect rationality, which, when applied out of context, may easily lead to unjustified enthusiasm.

[133] Arruñada*, Property Enforcement*, *supra* note 104, at 423–24.

[134] *Id.*

[135] *Id.* at 424–28.

[136] Indeed, "distributed ledgers naturally lend themselves to implementing high-level services that involve notaries, time-stamping, and high-integrity archiving, and promise to lower the costs of these activities by increasing automation, enabling easy switching of service providers, and peer transactions." U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 8 (2016), *supra* note 1, at 47. Note, however, that conveyancing, notarization, and data archiving are already partly decentralized, because they do not generally rely on central operators but on independent professionals' and parties' databases.

rights, also often called "land registration" or "title by registration" systems.[137]

First, to the extent that even in civil law jurisdictions notaries public are freely chosen by parties to private contracts, the blockchain will likely play a bigger role in notarization, even in real estate transactions.[138] The only functions for which notaries used to be clearly superior were for identifying parties and, more clearly, for ascertaining their legal capacity and serving as providers of settlement, closing, and escrow services for the parties.[139] These advantages, which for decades now have been under threat from complementary technological developments in identification and the related availability of registries for individuals' legal capacities, are now substantially affected by blockchain, as it has allowed the development of services that provide authentication and authorization, proving to other parties that you are who you say (authentication) and that you have the required permissions (authorization).[140]

[137] For an analysis of the different types of land registries, *see* Arruñada*, Property Enforcement*, *supra* note 104, at 406–23.

[138] See, for instance, in regard to the initiative being developed in the Republic of Georgia, Giulio Prisco, *BitFury Announces Blockchain Land Titling Project with the Republic of Georgia and Economist Hernando De Soto*, BITCOIN MAGAZINE (April 27, 2016, 10:56 AM), https://bitcoinmagazine.com/articles/bitfury-announces-blockchain-land-titling-project-with-the-republic-of-georgia-and-economist-hernando-de-soto-1461769012/.

[139] Benito Arruñada, *Market and Institutional Determinants in the Regulation of Conveyancers*, 23 EUR. J.L. & ECON. 93 (2007), argues that even civil law notaries face insurmountable difficulties to effectively review the legality of private contracts, providing a uniform quality of review. The main reason is that third parties, not being party to such contracts, do not influence the choice of notary. Even where notaries are organized as a closed shop, free choice of notary by parties introduces competition among them and, consequently, the actual level of review is that of the weakest link in the whole network of notaries, as shown by the lower quality and increased fraud observed after the liberalization of notaries in The Netherlands. Francien Lankhorst & Hans Nelen, *Professional Services and Organised Crime in the Netherlands*, 42 CRIME L. & SOC. CHANGE 163, 169–72 (2005).

[140] For a nuanced analysis of the authentication and authorization requirements, specifically developed to compare legacy and electronic conveyancing and titling systems, see Rod Thomas et al., *Australasian Torrens Automation, Its Integrity, and the Three Proof Requirements*, 2013 N.Z. L. REV. 227 (2013) and Rod Thomas et al., *Designing an Automated Torrens System — Baseline Criteria, Risks and Possible Outcomes*, 2015 N.Z. L. REV. 425 (2015). For an application to blockchain, see also Rod Thomas & Charlie Huang, *Blockchain, the Borg Collective and Digitalisation of Land Registries*, 2017 CONV. 14 (2017). The case of the Estonian government is particularly interesting:

Likewise, with respect to settlement, trade implemented through a blockchain can now provide conditioned simultaneous enforcement by using the principle of "atomicity," which, in essence, ensures that both parties fulfill their promises at the same time.[141]

Second, the applicability to registries of a truly decentralized blockchain (i.e., without trusted intermediaries) will be more limited because they play a public legal function, protecting the interests of unrepresented third parties and

> Since 2013, Estonian government registers — including those hosting all citizen and business-related information — have used Guardtime to authenticate the data in its databases. Their Keyless Signature Infrastructure (KSI) pairs cryptographic "hash functions" (see below) with a distributed ledger, allowing the Estonian government to guarantee a record of the state of any component within the network and data stores. . . .Using their ID card, citizens order prescriptions, vote, bank online, review their children's school records, apply for state benefits, file their tax return, submit planning applications, upload their will, apply to serve in the armed forces, and fulfill around 3000 other functions. . . . So how does a block chain help? It helps because every alteration of a piece of data is recorded. By providing proof of time, identity and authenticity, KSI signatures offer data integrity, backdating protection and verifiable guarantees that data has not been tampered with. It is transparent and works to the user's benefit too: citizens can see who reviewed their data, why, and when; and any alterations to their personal data must be authorised. Moreover, through using hash functions, as opposed to asymmetric cryptography used in most PKI, KSI cannot be broken by quantum algorithms. It is also so scalable that it can sign an exabyte of data per second using negligible computational and network overhead. It removes the need for a trusted authority, its signed data can be verified across geographies, and it never compromises privacy[.]

Alastair Brockbank, *Case Study – Estonian Block Chains Transform Paying, Trading and Signing*, in U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 83.

[141] This works in a similar manner to close a transaction:

> As long as the currency used for payment and the car ownership co-exist on the same block chain, Alice and Bob can form a single atomic transaction that simultaneously transfers ownership of the car and the payment for the car. Specifically, the transaction would specify two inputs: Alice's ownership and Bob's payment; and specify two outputs: the ownership to Bob and the payment to Alice. The transaction requires both parties to sign because both are providing inputs. If one signs and the other does not, the transaction is not valid. Once one party signs, the transaction details cannot be changed without invalidating the signature. Once the signed transaction is broadcast to the block chain, the car will wait for a preset number of confirmations (e.g., six) and then allow Bob access. Simultaneously, Bob's payment to Alice will be confirmed. One cannot happen without the other.

NARAYANAN ET AL., *supra* note 14, at 274.

therefore being much more than mere public databases.[142] Centralization and monopoly in registries are not rooted mainly in economies of scale but in the enhanced neutrality (not only with respect to parties to the contract but also with respect to strangers to it) required to reach universal legal effects.[143] However, this does not preclude that smart contracts could be complementary to property and company registries in many ways. For instance, property registries would be affected by the ability of applications such as Ethereum not only to register and track property but also to define new types of property entitlements, including multiple ownership claims and asset-sharing with sophisticated and nuanced allocations of use rights.

In principle, moreover, when considering the impact of blockchain on property registries, it is sensible to at least distinguish between recorders of deeds, such as those of France or the USA, and registers of rights, such as the German *Grundbuch* or the Torrens system of title by registration operating in Australia.[144] The latter not only date and keep the documents or "deeds" reflecting the transactions that the contractual parties agree to but also verify, as a necessary condition for entry into the register, that the intended transactions respect all other rightholders' rights on the specific asset.[145]

[142] Describing a land registry as a ledger is somehow misleading. Land registries are not standard ledgers. Systems based on the recordation of deeds merely time-stamp and archive documents and are therefore closer to a simple ledger. They are also similar to blockchains in that, in principle, they keep a record of the whole history of transactions, without purging possible contradictions. However, the date of entry at the registry holds crucial legal consequences, allowing the record to provide evidence on the priority of legal claims. Registries of rights are even more complex: they provide a sort of legal "balance sheet" defining not mere personal claims but the socially-accepted rights on a specific property. The "ledger" terminology focuses on the numeric or accounting personal aspect, while the key element in registries is social and legal: they do not mainly contain magnitudes (values) but the socially-accepted legal evidence supporting claims (recording) or even establishing rights (registration). If careful attention is not paid to this issue, attempts to apply blockchain in this area easily fall prey of the GIGO (that is, "garbage in, garbage out") principle. See, as an example, the account of the failed proposal to reform the land register of Honduras by Factom, provided by TAPSCOTT & TAPSCOTT, *supra* note 14, at 193–95. *See also* Rizzo, *supra* note 121.

[143] *See, e.g.*, TAPSCOTT & TAPSCOTT, *supra* note 14, at 194.

[144] ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 55–67.

[145] *Id.*

It is conceivable that a deed recordation system might be replaceable by an automatic system of dating private contracts and preserving their contents, if parties to private contracts cannot manipulate both functions once they sign their contract. However, even in that case, there is still a need for the law to establish the rules of evidence: to set the value of the blockchain as a source of evidence for in rem adjudication. For a blockchain to produce in rem effects, all parties must be obliged to express their will through it. Moreover, the law must trust those designing, putting in place, and—to some extent—governing, or at least affecting, the government of the blockchain system.

The official report of the pilot project carried out in Cook County (Chicago, Illinois) concurs with this analysis,[146] as it concludes that relying on an unpermissioned peer-to peer system would be too costly in terms of energy and would force most owners to rely on third parties,[147] seemingly inclining the report towards permissioned systems and to emphasize the use of blockchain for conveyance and lodging, but retaining the existing legal framework according to which "the county

[146] *See* KAREN A. YARBROUGH, COOK COUNTY RECORDER OF DEEDS, BLOCKCHAIN PILOT PROGRAM FINAL REPORT 32–34 (2017), http://cookrecorder.com/wp-content/uploads/2016/11/Final-Report-CCRD-Blockchain-Pilot-Program-for-web.pdf (last visited Sept. 16, 2017). The firm developing the system seems more optimistic: Ragnar Lifthrasir*, Permissionless Real Estate Title Transfers on the Bitcoin Blockchain in the USA! — Cook County Blockchain Pilot Program Report*, MEDIUM (Jun. 28, 2017), https://medium.com/@RagnarLifthrasir/permissionless-real-estate-title-transfers-on-the-bitcoin-blockchain-in-the-usa-5d9c39139292. A similar pilot, also limited to conveyancing, is reported by Matt Snow, *How I Sold 5 Acres of Land Using BitBay's Blockchain Smart-Contracts*, MEDIUM (Oct. 19, 2017), https://medium.com/@tradersnow/how-i-sold-5-acres-of-land-using-bitbays-trustless-smart-contracts-28f18b83125.

[147] The report agrees with our previous judgment that insufficient individual responsibility in preserving cryptographic keys would lead to reliance on trusted third parties:

> The Colored Coins (tokenization) approach seems to be a secure method for transmitting information, but it is complicated and requires users to become highly educated on how the technology works, including extremely secure and encrypted means for storing the private keys. Though securing a real estate transaction behind a password or private key would be a great way to prevent unauthorized transfers of property, it is not a stretch to imagine that such a system, if it required token reuse, would result in more people losing their private keys and requiring (another) third party to sell them back their key or perform a recovery action in a multi-signature transaction (e.g., 2 of 3 keys needed to sign).

YARBROUGH, *supra* note 146, at 33.

government record is the only *official* record."[148] In a similarly minimalistic vein, it considers that "tokenizing" title would pose substantial new legal challenges[149] and using digital signatures would facilitate secrecy and endanger the identification of participants.[150] Moreover, most of the positive aspects highlighted by the report are not exclusive of blockchain, such as the possibility of combining conveyance and recordation into a single event, using separate components of blockchain components to improve current recordkeeping practice (in particular, Cook County has decided to add file hashing and data integrity certification), consolidating property information currently spread across several government offices in a single website, and making fraud harder by protecting conveyances with cryptographic keys.[151]

Blockchain may also lower the costs of identifying rights and assets, making new types of registers viable, enabling finely-tuned solutions for more detailed rights in intellectual property and completely new registries for certain high-value assets, as suggested by the Everledger initiative for registering diamonds and other specially valuable assets.[152] Note in this regard that private ordering arrangements enjoy an advantage when rights are unenforceable in rem, as with assets that are "easily portable, universally valuable and virtually untraceable," such as diamonds, which explains why the diamond industry has been based on a "millennia-old distribution system that relied on multiple layers of personal exchange."[153] Blockchain would alter this advantage if it is capable of relaxing this constraint, so that it becomes economically viable to identify each individual asset,

[148] *Id.* at 22 (emphasis in original).

[149] *Id.* at 39–40.

[150] *Id.* at 38–39.

[151] *Id*. at 34–38.

[152] Natasha Lomas, *Everledger Is Using Blockchain to Combat Fraud, Starting with Diamonds*, TECHCRUNCH (June 29, 2015), https://techcrunch.com/2015/06/29/everledger/.

[153] Barak D. Richman, *Ethnic Networks, Extralegal Certainty, and Globalisation: Peering into the Diamond Industry*, *in* CONTRACTUAL CERTAINTY IN INTERNATIONAL TRADE: EMPIRICAL STUDIES AND THEORETICAL DEBATES ON INSTITUTIONAL SUPPORT FOR GLOBAL ECONOMIC EXCHANGES 31, 32 (Volkmar Gessner ed., 2009).

this being one of the stated objectives of the Everledger registry.[154]

B. COMPANY REGISTRATION

The case of company registries is similar to that of recordation of deeds, to the extent that most company registries are closer to recordation than to registration systems. However, company registries could be challenged by initiatives like the Ethereum blockchain, as these aim to create virtual decentralized and autonomous organizations that would be defined only by a given set of rules running in the blockchain. In principle, these organizations can be flexibly organized, allocating specialized managerial and contractual functions in different manners.[155] However, a historical perspective throws light on the potential contribution and likely difficulties of this contractual approach to company incorporation. The experience of the English "unincorporated companies" prior to the creation of the English Company Registry in 1844 provides relevant insights.[156] In general terms, they suggest that, even assuming perfect immutability of the blockchain, the explicit backing of the law and judicial rulings seem indispensable to avoid future conflict ex post and to provide parties with the necessary certainty ex ante.

A less ambitious initiative is the development of an international standard for the identification of legal entities, known as the Register of Legal Organizations (ROLO).[157] It is revealing that, despite being led by collaborative industry, given that most transactions are business-to-business (B2B), what is

[154] Lomas, *supra* note 152; *see also* U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 8 (2016), *supra* note 1, at 56.

[155] *C.f.* Abramowicz, *supra* note 48, at 414 ("The traditional forms of business association differ in how they allocate ownership interests and decision-making authority, but the peer-to-peer business association allocates decision-making authority in a new way—not to a specific owner, to partners, to a board, or even to shareholders, but to the peer-to-peer decision-makers as a whole.").

[156] See generally RON HARRIS, INDUSTRIALIZING ENGLISH LAW (2000), for the historical evidence. For an interpretation along the lines of the text, see Benito Arruñada, *Institutional Support of the Firm: A Theory of Business Registries*, 2 J. LEGAL ANALYSIS 525, 558–62 (2010).

[157] *See* Andrew Coakley, *The Block Chain Network: Accelerating Adoption*, SOPRA STERIA 5 (2016), http://www.slideshare.net/AndrewCoakley1/blockchain-final-25112015-v11.

being considered is the need for ROLO "in each nation,"[158] and the expected presence of a mandatory element. In particular, "enrolling into a ROLO at a Level of Assurance is voluntary; however, being in ROLO will become mandatory for future high assurance identity federation, cyber assurance and insurance requirements. It can also be expected to become mandatory for government contractors and companies in a number of regulated sectors."[159] In England, it has the support of Companies House, the English company register.[160]

Blockchain implications are clearer in other corporate areas that are intrinsically contractual. For instance, blockchain has the potential to automatize transactions in the area of "corporate actions": any announcements made by a public company affecting its securities and which may require an action by either investors or their representative agents. Examples include dividends and coupon payments, offers to issue or redeem securities,[161] stock splits, mergers, and spin offs. Most of this data is communicated to investors through a complex channel involving suppliers of financial data, securities' custodians, and investment fund managers, who then also carry investors' decisions in the opposite direction.[162] In both directions, blockchain could make the whole process much more efficient and automatic.[163]

[158] *Id.*

[159] *Id.* at 6.

[160] *Id.* ("ROLO's design is being industry led and has gained some early support from a wide range of industries, including those already covered by Companies House (including Companies House itself).").

[161] Trading shares on a blockchain is legal in Delaware since July 2017. Michael del Castillo, *Delaware House Passes Historic Blockchain Regulation*, COINDESK (July 1, 2017), https://www.coindesk.com/delaware-house-passes-historic-blockchain-regulation/.

[162] On the considerable costs and risks, both actual and potential, of these systems, see the report sponsored by the Depository Trust & Clearing Corporation and produced by Oxera. *Corporate Action Processing: What Are the Risks?*, OXERA i–ii (2004), http://www.oxera.com/Oxera/media/Oxera/downloads/reports/Corporate-action-processing.pdf?ext=.pdf (estimating at one million the number of corporate actions worldwide, and further estimating the annual risk at between 1.6 and 8 billion Euros and annual actual losses at between 300 and 400 million Euros).

[163] *See* Dominic Hobson, *Case Study 2 — Corporate Actions*, *in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 58–59 ("In theory, [blockchain technology] could eliminate all intermediaries between the issuer and the fund manager, guaranteeing the accuracy and timeliness of the information.").

C. PROPERTY REGISTRATION

All registries of rights (often called "title" or simply "registration" systems) include a registry of documents in the form of their lodgment book, which they use to establish priorities before undergoing registration review. What has already been said about recordation systems applies to this part of registration systems.

In addition, in comparison with property recordation and company registries, property registries of rights should be less affected by blockchain, to the extent that registration review cannot be easily exercised by an automatic system (even a centralized one): it would be facing similar difficulties to those considered above with respect to contractual completion. The standard historical solution when creating modern land registries has been to reduce the variety of rights enforceable in rem, defining a smaller and closed number of in rem rights (the "numerus clausus" principle),[164] and to make property transactions more "abstract" (i.e., formal). This simplification of property rights is worthwhile to the extent that it makes it possible for registries of rights to function or, in general, reduces information asymmetries in markets.[165] However, it may also be costly because a smaller set of rights benefits from the advantages of being enforced in rem. In this vein, the proposal to have part of the transaction "out of the blockchain" (as in Blockstack's simple contracts, described in note 76) might end up creating a two-step transacting process broadly similar to the separation between the "causal" and "abstract" stages present in many legal systems but most clearly established in German property law.[166]

[164] *See generally* Merrill & Smith, *supra* note 3; Hansmann & Kraakman, *supra* note 3; Arruñada*, Property Enforcement*, *supra* note 104.

[165] For an empirical test of the role of the numerus clausus in different types of registries, see Arruñada*, Property Enforcement*, *supra* note 104, at 416–23.

[166] *See* Jürgen Kohler, *The Law of Rights in Rem*, *in* INTRODUCTION TO GERMAN LAW 227, 231 (Werner Ebke & Matthew W. Finkin eds., 1996) (describing how the principle of abstraction or *Abstraktionsprinzip* that is characteristic of German property law makes transactions concerning property rights formal and abstract, and showing how transactions take place by entry into the land register or *Grundbuch* and are valid irrespective of the validity of the causal obligation); *see also Off-Chain Transactions*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Off-Chain_Transactions (last visited Oct. 12, 2017) (explaining that the separation between on-chain and off-chain transactions—

Moreover, in a fully decentralized system of property, all individuals would take care of their rights by themselves, as the rules of evidence used to establish title need to be the same for all parties holding rights in that type of asset. They would need to keep their cryptographic keys and to decide about any transaction that other individuals propose which might affect their rights. As mentioned previously, many individuals, probably the majority, prefer to rely, at least partly, on trusted private and institutional intermediaries.

Proposals to apply blockchain in the registration of real property confirm this analysis. For instance, the above-mentioned Swedish *White Paper* provides a valuable illustration as, in essence, it is limited to reorganizing the in personam contractual process precedent to the in rem property transaction. The changes proposed in Sweden thus resemble the "Landonline" system of electronic conveyancing and registration implemented in New Zealand since 2009,[167] but with a key difference: the Swedish Land Register would at least initially retain all its powers to review and decide on registration: "In an initial stage, the database of Lantmäteriet remains intact. Updates to the land registry are retrieved from the blockchain and are then also checked by Lantmäteriet. Registration in the blockchain is digital and based on the legal requirements, which minimizes errors in the information."[168] Moreover, the land

used to speed them up, save fees and scale systems more easily—can be interpreted in this vein).

[167] The changes proposed in Sweden are summarized at KEMPE, *supra* note 24, at 27–31. *See also* Alex Mizrahi, *A Blockchain-Based Property Ownership Recording System*, CHROMAWAY, 2016, http://chromaway.com/papers/A-blockchain-based-property-registry.pdf (discussing the challenges of "implementation of blockchain-bnased [sic] property ownership recording system[s]"); *Blockchain and Future House Purchases: Second Phase Completed in March 2017*, CHROMAWAY, http://chromaway.com/landregistry/ (last visited Oct. 27, 2016) (providing an interactive demonstration of a property purchase using blockchain technology). For a description and analysis of the New Zealand case, see Benito Arruñada, *Leaky Title Syndrome?*, 2010 N.Z. L.J. 115 (Apr. 2010). For a more general discussion of electronic conveyance see ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 208–15.

[168] KEMPE, *supra* note 24, at 33. As imagined, the interaction of the blockchain with the land registry would be minimal:

> The blockchain for the transactions is open source and is checked by Lantmäteriet, but can be verified by anybody. The chain of authorization, signing with a Telia ID, etc. can be edited. The blockchain saves the verification records of documents such as the bill of sale and the purchasing contract. Storing the original documents and their verification records can be performed by an external party,

register also defines the assets and (supposedly) the authority to deal:

> A central part of the practical application of blockchains is the identification of what the digital codes will represent in the physical world. As described above, it is LHV Bank, Lantmäteriet or someone else behind a solution that is the organization that determines what the digital codes represent and who is authorized to transfer or act in a contracts [sic]. In other words, Lantmäteriet guarantees which digital representation a specific property has.[169]

Therefore, the only substantial change proposed in the *White Paper* seems to be the development of a seemingly private blockchain application for electronic conveyance, which would make it possible for all parties involved to work with the same information, expanding their knowledge and reducing duplications and mistakes.[170] A benefit would be that, through the application, all parties would also have instant access to any filing in the register that may affect the legal standing of the rights being traded.[171]

On the other hand, the system is planned to work with "pending property titles" during the whole conveyance process until eventual registration, which the *White Paper* hopes would always be granted by its assumption that registration refusals are now mainly caused by bureaucratic mistakes: "The risk that

> but can also be stored digitally by each party in the agreement, the bank, buyer, seller, agent, etc. The documents and verification records are then stored in multiple locations, which creates redundancy. The verification records are also recorded in an external blockchain, which means that all of the parties can feel secure that they can re-create and demonstrate the chain of events on their own, in the event that the other parties suffer a breach of data or similar event.

Id. Moreover, "the land registry of Lantmäteriet is, in principle, entirely separate from the solution." *Id.* at 34. Some less ambitious projects only use the blockchain as a data depository for the current register. *See, e.g.*, Ian Allison, *Blockchain-Based Ubitquity Pilots with Brazil's Land Records Bureau*, INT. BUS. TIMES (Apr. 5, 2017), http://www.ibtimes.co.uk/blockchain-based-ubitquity-pilots-brazils-land-records-bureau-1615518.

[169] KEMPE, *supra* note 24, at 22. For the related problem of guaranteeing who is authorized to transfer, this Swedish initiative seems to rely on mobile phone identification:

> Another central part is the identification of the actors who will have rights to act in the system. For this, a secure ID solution is required. This solution also needs to be easily accessible to the actors involved. If we look to the future, we see a world where mobile phones play an increasingly important part in the ID solutions being developed.

Id.

[170] *Id.* at 26.

[171] *See supra* notes 152–54 and accompanying text.

the property title will not be granted is sharply reduced since the system can ensure that the information that is required by law is included in the system and is required by the system in order for the parties to be able to provide their signature."[172]

However, even if most refusals have been rooted in bureaucratic errors, it is likely that the important refusals in terms of value and legal security will be those that impede dubious or even fraudulent transactions from damaging third parties.[173] In principle, it is unclear how they would be affected by the new system. If this analysis is correct, two important consequences follow. First, what is mentioned above about the "initial" functions to be played by the land register in a supposedly transitional period would likely become a permanent feature of the system. Otherwise, there is a risk of inadvertently transforming a register of rights or registration-of-title system into a recordation-of-deeds system.[174] Second, speeding up the whole process and maintaining the same level of legal security likely requires introducing at earlier stages an advanced registration review. The "pending" titles repeatedly mentioned in the *White Paper* would then be upgraded to "conditional" property titles.

VI. CONCLUDING REMARKS ON FIRMS, CONTRACTS AND PROPERTY

Blockchain is said to be "trustless,"[175] pointing out that it does not need trust to work. However, this trustless feature needs to be qualified. Blockchain and other institutional and physical technologies supporting more impersonal exchange in fact replace trust *between* counterparties with all parties' trust *towards* some third-party intermediary, be it a register, an organized exchange, a bank, a credit card system, etc.[176] Blockchain enthusiasts claim that it gets rid of intermediaries but this claim proves illusory: it is more a Holy Grail than a

[172] KEMPE, *supra* note 24, at 32.

[173] *See*, *e.g.*, *supra* notes 81–82 and accompanying text.

[174] ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 210–12.

[175] *See*, *e.g.*, Nikunj Jain, *Blockchain: Why a Trust-Less System is the Most Trustable System in the World*, CRYPTOCOINS NEWS (Apr. 21, 2017), https://www.cryptocoinsnews.com/blockchain-trust-less-system-trustable-system-world/.

[176] *See* discussion *supra* note 36.

realistic objective.[177] The paper shows the major roles played by different types of intermediaries. Their presence holds key consequences for specialization opportunities, firms' strategies, and the structure of contracting and property processes:

First, blockchain applications will tend to rely on dual structures of causal and formal transactions,[178] with the formal stage being highly abstract, using simple contracts and enforcing a closed number of property rights. This excludes the possibility of enforcing a wider variety of rights in rem.[179]

Second, the core peer-to-peer structure of blockchain faces insurmountable difficulties to reach contractual completion and to interact with the real word,[180] two difficulties that have been framed here in terms of, respectively, contract (in personam) rights and property (in rem) rights.

Third, to overcome these difficulties and to complement its core peer-to-peer structure, blockchain development will encourage the proliferation of a myriad of new specialists to provide effective contractual completion as well as interfaces between the virtual and real worlds to most end users and for most assets.[181]

Fourth, the emergence of specialized agents will reduce some costs at the price of increasing agency costs, therefore creating additional conflicts of interests. This will open up additional opportunities for fraud and trigger greater demand for centralized and specialized enforcement and regulation.[182]

More generally, because of the role of intermediaries, blockchain is likely to affect transaction costs in all types of transactions, modifying the comparative advantages of different organizational forms and institutions, e.g., the optimal degree of vertical and horizontal integration in business firms and other organizations, and even the relative optimal scope of markets and politics as information, decisional, and allocation mechanisms. However, not only the extent but also the signs of these impacts are open to question. Therefore, contrary to

[177] *See* discussion *supra* note 36.

[178] *See*, *e.g.*, *supra* note 166 and accompanying text.

[179] *Supra* note 164 and accompanying text.

[180] *See*, *e.g.*, *supra* note 131 and accompanying text.

[181] *See*, *e.g.*, *supra* notes 36–37 and accompanying text.

[182] *See supra* notes 93–96 and accompanying text.

common assertions, it is debatable if blockchain really favors market transactions over business firms, and to what extent.[183]

Lastly, blockchain will find it easier to enable transactions in personal (i.e, contractual, in personam) rights as compared to real (i.e., property, in rem) rights. To move from the world of personal rights to the world of real rights will require public interfaces and interventions (at the very least, to establish the status of the blockchain as judicial evidence). Therefore, applications of blockchain in property transactions will likely be limited to document notarization and the conveyance of small-stakes and possession-based transactions, as well as to, at the most, the use of private blockchains for archiving purposes within standard registration systems.

[183] For instance, TAPSCOTT & TAPSCOTT, *supra* note 14, at 142, claim that "as technology continues to drop costs in the market, it's conceivable that corporations could and should have very little inside—except software and capital"). The analysis here points out that powerful forces also operate in the opposite direction: mainly, the emergence of new contractual specialists, who in most cases will likely be organized as business firms instead of acting as individuals.

***