

BLOCKCHAIN'S STRUGGLE TO DELIVER IMPERSONAL EXCHANGE

BENITO ARRUÑADA*

ABSTRACT

With its decentralized peer-to-peer structure, application of the blockchain technology underpinning Bitcoin holds the promise of making impersonal exchange possible for all types of old and new transactions in all types of markets. Such theoretical promise is examined here by identifying what value blockchain adds to the contractual process, exploring its contractual potential and analyzing the main difficulties it is facing.

The article argues that blockchain applications will evolve towards dual structures separating causal and formal transactions. Contrary to naive conceptions that proclaim the end of intermediaries and state involvement, such applications will rely on a variety of interface and enforcement specialists, including standard public interventions, especially for property transactions. Without these interventions, blockchain will at most work as an in personam—instead of as an in rem—system, therefore facilitating mere personal instead of impersonal transactions.

* Professor, 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, Teófilo Hurtado Navarro, Eduardo J. Martínez García, Fernando P. Méndez González, Nicolás Nogueroles Peiró, Rod Thomas and Jacques Voss, as well as the assistance of Ian Todd. It received support from the Spanish Ministry of the Economy and Competitiveness through grant ECO2014-57131-R. Usual disclaimers apply.

CONTENTS

I. Introduction	3
II. A brief on blockchain and “smart contracts”	4
A. The nature of blockchain.....	4
B. Smart contracts	6
III. Blockchain and contract, <i>in personam</i> , rights	8
A. The presence of central enforcers	10
B. Contract completion in smart contracts.....	14
IV. Blockchain and property, <i>in rem</i> , rights.....	17
A. The need for interfaces between personal and real rights.....	17
B. Insights from the theory of property rights	21
V. Assessing blockchain applications in property.....	24
A. Private blockchains and “legacy” systems.....	24
B. Conveyancing and property titling.....	26
C. Company registration	28
D. Property registration.....	29
VI. Concluding remarks on firms, contracts and property	31

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 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 distinction between private and

¹ For instance, a report by the UK Government claimed that it “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.” Mark Walport, *Executive Summary and Recommendations*, in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 8 (Mark Walport ed., 2016), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (last visited Sep. 8, 2016).

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, BLOCKCHAIN ADOPTION IN CAPITAL MARKETS 6 (2016), available at <https://www.greenwich.com/fixed-income-fx-cmds/blockchain-adoption-capital-markets> (last visited Dec. 4, 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.

³ 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).

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 to frustrated expectations. This is not a new problem, however, as land titling and administrative simplification efforts have been suffering similar problems for the same reason.⁷ 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. 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. Traditional payment

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

⁵ For instance, Christian Catalini & Joshua S. Gans, *Some Simple Economics of the Blockchain* (Nat'l Bureau of Econ. Research, Working Paper No. 22952, 2016), available at <http://www.nber.org/papers/w22952>.

⁶ 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.

⁷ 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.

systems solve these problems by relying on central, specialized and trusted third parties such as banks, payment systems, credit card companies and clearing houses. In contrast, the blockchain solved them with a peer-to-peer solution. 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. To achieve this feat, it replicates the ledger in a multitude of computers or “nodes”, making all the history of transactions public, accessible and widely distributed across the whole network of users.⁸

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. 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),⁹ 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.

⁸ For more detailed explanations, see the descriptions in Rainer Böhme, Nicolas Christin, Benjamin Edelman, & Tyler Moore, *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSP. 213, 215–19 (2015); Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 576–88 (2015); 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 a reliable technical introduction, ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* (2016), whose draft is available at https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1; or the abundant specialized literature, even though it tends to exaggerate its potential—e.g., WILLIAM MOUGAYAR, *THE BUSINESS BLOCKCHAIN: PROMISE, PRACTICE, AND APPLICATION OF THE NEXT INTERNET TECHNOLOGY* (2016) or DON TAPSCOTT & ALEX TAPSCOTT, *BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD* (2016); as well as, for a simpler description, *The Great Chain of Being Sure about Things*, *ECONOMIST*, Oct. 31, 2015, at 19 [hereinafter *The Great Chain of Being Sure about Things*].

⁹ However, 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.

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

The system motivates these miners by paying them when they create a new block (e.g., 25 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.

The system is protected against tampering and revision by duplication of the blockchain in many computers and concatenation of any subsequent blocks,¹⁰ 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). The header is easy to produce on the basis of the information in the chain. Therefore, if the chain's contents were modified, the change would cause an easily observable discrepancy, and the latest block would be rejected. (In registry terms, entry or filing would be denied).

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. Therefore, a malevolent *A* would need to lengthen the chain faster than all other users, which in principle would require *A* to control more than half of the network's computers.¹¹

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.¹² Therefore, blockchain

¹⁰ On the potential benefits of the costly solution of having redundant repositories of information, see Matthew C. Stephenson, *Information Acquisition and Institutional Design*, 124 HARV. L. REV. 1422, 1462–75 (2011).

¹¹ See JOSHUA A. KROLL, IAN C. DAVEY, & EDWARD W. FELTEN, *THE ECONOMICS OF BITCOIN MINING, OR BITCOIN IN THE PRESENCE OF ADVERSARIES*, (2013), available at <http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf> for 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." *Id.* at 1. See, for more detailed information, MAGNUS KEMPE, *THE LAND REGISTRY IN THE BLOCKCHAIN* 34 (July 2016) (on file with author).

¹² For instance, to mention only a few applications, Colu claims to provide a tool for creating local economies, including the issuance of digital currencies (<https://www.colu.com/>); Factom tried to provide a prototype of land registry based on the blockchain to the Honduras' Property Institute; Everledger is implementing a fraud-prevention registry of luxury goods such as diamonds, which, by recording their distinguishing attributes, would help provide proof of

technology is now applicable not only to payments but to all sorts of contracts relying on trust. Understandably, it is often defined as a “trust machine” because it “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.”¹³

Its most ambitious application 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.¹⁴ (Video-on-demand and ATMs could be seen as simplistic antecedents.) In a way, they use the blockchain ledger as their enforcement mechanism,¹⁵ so that transactions are supposed to be conclusive or “immutable”.

identity in case of theft (<http://www.everledger.io/>); Blockstack allows registration of identities, public keys and names in the blockchain, providing more security than traditional identity, naming, and digital registries (<https://blockstack.org/>); and 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” (<http://coinspark.org/>). Keep in mind, however, 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. KEMPE, *supra* note 11, at 11–12, 15.

¹³ Therefore,

the blockchain [. . . is, in essence,] 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. . . . The real innovation [behind bitcoin] is not the digital coins themselves, but the trust machine that mints them—and which promises much more besides.

The Trust Machine, ECONOMIST, Oct. 31, 2011, at 11.

¹⁴ Nick Szabo, *The Idea of Smart Contracts*, MANUSCRIPT (1997) http://szabo.best.vwh.net/smart_contracts_idea.html (last visited Aug. 1, 2016).

¹⁵ Kiviat, *supra* note 8, at 605. Decentralized smart contracts are understood as “contracts that leverage a secure public ledger as an enforcement mechanism.” *Id.* 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 authenticity.” *Id.* at 603. Added conditions could reflect the parties’ desire that the transaction occur only under certain circumstances or at a certain time, etc. The term, “smart contract” was 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

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.¹⁶

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 network, *without trusted or necessary*

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.

Nick Szabo, *The Idea of Smart Contracts*, http://szabo.best.vwh.net/smart_contracts_idea.html (last visited Aug. 1, 2016). *See also* Nick Szabo, *Secure Property Titles with Owner Authority*, <http://szabo.best.vwh.net/securetitle.html> (last visited Aug. 10, 2016). Many initiatives are currently developing to implement smart contracts, from the very simple to the most complex. 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.*, about Lighthouse Partners at <http://www.lighthouse-partners.com/>, (last visited Aug. 18, 2016).

¹⁶ For example, a major Australian law firm concludes that

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), *available at*, <http://www.allens.com.au/data/blockchain/index.htm?sku=fsdah5e556eqweqwg> (last visited Oct. 27, 2016).

intermediaries".¹⁷ In particular, smart contracts are supposed to work without third party intervention, which should avoid the risk that the trusted party or a government with power over it might be in a position to manipulate the content of the ledger. To this extent, they could, therefore, be understood as a paradigm of pure private ordering.¹⁸

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.¹⁹ For instance, they may require other agents, such as "oracles", to monitor external or "off-blockchain" information on 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.²⁰ Even the dependence on oracles is thought to "undermine the goal of agreements free of human caprice."²¹ And it is undeniable that curators add some degree of centralization and specialized enforcement.²²

¹⁷ Phil Godsiff, *Disruptive Potential*, in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 61 (emphasis added). Similarly, the co-founder of the digital asset exchange Coinbase claims that "we will no longer need central companies to act as the middleman" Fred Ehrsam, *How the Blockchain Could Change Corporate Structure*, WALL ST. J., Oct. 19, 2016, <http://www.wsj.com/articles/how-the-blockchain-could-change-corporate-structure-1476887998>.

¹⁸ Blockchain has even been considered by Libertarians as a means to get rid of the state altogether. Tapscott & Tapscott, *supra* note 8, at 199–201.

¹⁹ For the distinction between property (*in rem*) and contract (*in personam*) rights, see Merrill & Smith, *supra* note 3; and Hansmann & Kraakman, *supra* note 3. About its economic consequences, ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 15–34; Arruñada, *Coase and the Departure from Property*, *supra* note 4, at 305–19.

²⁰ *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 (Aug. 3, 2016, 11:04 AM), available at <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>.

²¹ *Not-so-clever contracts*, ECONOMIST, July 28, 2016, available at <http://www.economist.com/news/business/21702758-time-being-least-human-judgment-still-better-bet-cold-hearted> [hereinafter *Not-so-clever contracts*].

²² For instance, in the DAO case analyzed next in section 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 20. Ethereum claimed that "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" ("Protecting the DAO," available at <https://daohub.org/curator.html>). It is true that curators only perform two functions: (1) "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)" and (2) "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

A. *The presence of central enforcers*

More revealingly, smart contracts may even require enforcers in a more traditional sense, related to contract completion.²³ 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.²⁴ The DAO (the acronym stood for “Decentralized Autonomous Organization”) was a sort of venture capital fund to which any investor could contribute “ether”, the Ethereum’s cryptocurrency, thus purchasing shares and voting rights, which they then used on the projects they decided to support.

author of the Proposal, thereby confirming the author of the Proposal” (“Task,” <https://daohub.org/curator.html>). Moreover, these two functions are also performed by token holders, who on the other hand are fully responsible for evaluating proposals; auditing their smart contract code; providing them with legal advice, if any; and taking economic responsibility for them (<https://daohub.org/curator.html>). However, their enforcement role became evident during evolution of the venture. (All sites in this footnote were visited on August 12, 2016).

²³ Even Bitcoin works with a substantial degree of human rulemaking:

the 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 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, in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 43.

²⁴ Ethereum is the brainchild of Vitalik Buterin, was crowdfunded in August 2014 and developed by a Swiss nonprofit Foundation. See its foundational manifest (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)) and “Homestead Documentation” (Ethereum, *Ethereum Homestead Documentation*, <http://www.ethdocs.org/en/latest/> (last visited Aug. 1, 2016)).

Ethereum understands smart contracts as “applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference”. These applications

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*.²⁵

The DAO therefore aimed to implement the “code is law” principle coined by Lessig,²⁶ according to which the code itself provides conclusive enforcement.²⁷ However, the incident showed that implementing this principle is harder than it seemed, as the hacking of the contract led to its subsequent revision, showing that its terms were not conclusive and the blockchain was not immutable. 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 “take” from its original owners about \$60 million worth of ether.²⁸ At that point,

²⁵ ETHEREUM HOMESTEAD RELEASE: BLOCKCHAIN AND PLATFORM, <https://www.ethereum.org/> (last visited Aug. 2, 2016) (emphasis added). It also encourages users to “create 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 will be automatically compatible with any wallet, other contract or exchange also using this standard.”

²⁶ LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999); LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

²⁷ A narrower version 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 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>.

²⁸ Paul Vigna, *Ethereum Gets Its Hard Fork and the ‘Truth’ Gets Tested*, MONEY BEAT, WSJ BLOG (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.

The Attacker, *An Open Letter: To the DAO and the Ethereum Community*, PASTEBIN, (June 18, 2016), <http://pastebin.com/CcGUBgdG> (emphasis added).

the Ethereum team decided to implement a “hard fork” which, if adopted by its community of users, would effectively delete the fraudulent transactions and refund the stolen money to its previous owners but endangering the conclusiveness of the contracting process.²⁹ 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.”³⁰

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.³¹ 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.”³² Some degree of centralization was made visible by the promoters’ power to manage the system. Moreover, their ability to do so hinted that the risk of similar interventions was present in all other blockchain applications.

Consequently, the community was split and important miners and exchanges started backing an alternative currency, called “Ethereum Classic,” that uses the original blockchain, with those who held ether on it retaining their rights but for the funds stolen in the DAO attack.³³ Their goal was to preserve the immutability of the blockchain and

²⁹ Note that

a hard fork in the rules concerning a valid block *occurs only when the new rules would result in acceptance of blocks that the old rules would reject*. . . . With a 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) (emphasis added) David Kirk, *Cryptocurrency: What is a Fork?*, Tech-Recipes (Mar. 11, 2014), <http://www.tech-recipes.com/rx/48517/cryptocurrency-what-is-a-fork/> and *Bitcoin Developer Guide: Consensus Rule Changes*, Bitcoin, <http://www.bitcoin.org/en/developer-guide#consensus-rule-changes>).

³⁰ 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>.

³¹ Shea continued:

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.

Id. The key issue is, in these terms, that the hard fork treated them as social contracts.

³² Aytar Sehra, *Building a Decentralised Ecosystem*, slide 9 (2016), available at <http://www.slideshare.net/arcatomia/ethereum-classic-18-august-2016>.

³³ In detail:

the conclusiveness of transactions, even if the claims of code-as-law are 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.”³⁴ Ethereum Classic immediately became the third most traded cryptocurrency behind bitcoin and the hard fork version of ether.³⁵ Some months later, it looked relatively strong,³⁶ a remarkable achievement considering that it had suffered numerous attacks.³⁷

However, despite Ethereum Classic being presented as a decentralized, non-governed blockchain system, this alternative to the hard fork also relied on third-party enforcement, only in the more conventional form of state intervention. As argued by an organizer of Ethereum Classic, the solution for failures should be based on “[l]egal 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.”³⁸ It can be concluded that, at least for fraud cases, ETC relies on standard legal recourse and blockchain integrity is dissociated from self-enforcement. 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

Because the funds were locked up in The DAO, developers were able to “lock” the funds until The DAO was scheduled to release its funds to the participants. Slock.it cancelled The DAO and a hard fork was created to return the stolen funds. The plan was to make it as if The DAO itself, including the hack, had never happened. This course of action angered a significant minority of the community, who insisted that it was more important that the Ethereum blockchain remain immutable.

That group of miners continued to mine of the original (pre-fork) chain, essentially creating a new coin dubbed Ethereum Classic. By continuing on the non-forked chain, they essentially created two worlds: one where The DAO, along with all the consequences of its hack, still existed, and one where it never happened.

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>.

³⁴ Sehra, *supra* note 32, at slide 10.

³⁵ 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/>.

³⁶ For example, on October 17th, 2016, the market capitalization of Ethereum Classic was approximately 9.33% that of Ethereum and in the last 30 days it had been the fifth most traded cryptocurrency, with 16.46% the volume of Ethereum (calculated by the author with data obtained from <https://coinmarketcap.com/>).

³⁷ See Jamie Redman, *A Victorious Rebellion? Microsoft Investigates Ethereum Classic’s Potential*, BITCOIN.COM (Sep. 27, 2016), <https://news.bitcoin.com/microsoft-looks-rebel-ethereum-classic/>.

³⁸ Sehra, *supra* note 32, at slide 10.

“dogmatic application of immutability” that had been the main reason to create this new cryptocurrency in the first place.³⁹

B. Contract completion in smart contracts

The case teaches some important general lessons. Furthermore, being a controversial case, it shows 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.⁴⁰

Second, as in other attempts to enable impersonal exchange, it makes sense to argue for contract (and property) simplicity. The root of the DAO problem was that smart contracts faced the old tradeoff between security and complexity,⁴¹ and have to operate in an uncertain and changing environment that emphasizes the need for adaptation. Furthermore, errors in computer code are prevalent and impossible to eradicate, and they

³⁹ Andrew Quentson, *Ethereum Classic Divided Over the Proposed Hardfork*, CRYPTOCOINS NEWS (Oct. 14, 2016), <https://www.cryptocoinsnews.com/ethereum-classic-divided-proposed-hardfork/>.

⁴⁰ 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 his theft 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.

What is Ethereum Classic, *supra* note 20 (punctuation modified by the author).

⁴¹ Shea, *supra* note 30.

increase with complexity,⁴² 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”, which also points to centralization. Shea therefore recommends “simple contracts” based on making contract code as simple as possible, running most of the logic off the chain and upgrading it by the majority of the parties.⁴³

This argument for simplicity also resonates with the old effort in property law to define a smaller and closed number of in rem rights (the “*numerus clausus*” principle⁴⁴) and to more “abstract” (i.e., formal) transactions. Similarly, the proposal to have part of the transaction “out of the blockchain” (as in Shea’s simple contracts) might end up creating a two-step transacting process broadly similar to the separation between the “causal” and “abstract” stages in German property law.⁴⁵ A somehow similar 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.”⁴⁶

⁴² 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 “on average, software comes with between 15 and 50 defects per 1,000 lines of code.” *Not-so-clever contracts*, *supra* note 21.

⁴³ This would be implemented by (1) “encoding minimal logic on the blockchain”, which would only define the parties to 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) having parties running the code off of the chain and submitting transfer requests which go through when accepted by a majority of parties running the code. Shea, *supra* note 30 (emphasis added).

⁴⁴ See, on this, Merrill & Smith, *supra* note 3; Hansmann & Kraakman, *supra* note 3; and Benito Arruñada, Property Enforcement as Organized Consent, 19 J.L. ECON. & ORG. 401 (2003) [hereinafter Arruñada, *Property Enforcement*].

⁴⁵ The principle of abstraction or *Abstraktionsprinzip* that is characteristic of German property law makes transactions concerning property rights formal and abstract. Jürgen Kohler, *The Law of Rights in Rem*, in INTRODUCTION TO GERMANY LAW 227, 231 (W. F. Ebke and M. W. Finkin, eds., 1996). They take place by entry into the land register or *Grundbuch* and are valid irrespective of the validity of the causal obligation. I will come back below to the issue of abstraction when analyzing the application of the blockchain to land registers.

⁴⁶ Abramowicz, *supra* note 29, at 362 (notes 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, in the same way that other open source projects are. *Id.* at 367.

Blockchain adds value by providing verifiability on the *content* of contractual documents. However, it is doubtful 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 blockchain on relational contracts are likely to be small, whatever the “relational” concept used. Blockchain is unlikely to affect relational contracts if by “relational” we mean contracts that are completed by the parties *ex post*, sometime in the future after they committed to the contract.⁴⁷ 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. Similarly, availability of blockchain should not affect 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.⁴⁸

The role of simplicity and the *numerus clausus*—i.e., the scope for *ex ante* completion—helps explain why blockchain seems to be gaining more ground in the financial world and, in particular, in such areas as derivatives trading,⁴⁹ 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 faster in low-value contexts.⁵⁰

⁴⁷ In the vein of OLIVER E WILLIAMSON, *THE ECONOMIC INSTITUTIONS OF CAPITALISM: FIRMS, MARKETS, RELATIONAL CONTRACTING* (1985).

⁴⁸ In the spirit of Benjamin Klein & Keith B. Leffler, *The Role of Market Forces in Assuring Contractual Performance*, 89 J. POL. ECON. 615 (1981); and Carl Shapiro, *Premiums for High Quality Products as Returns to Reputations*, 98 Q.J. ECON. 659 (1983).

⁴⁹ See, for instance, the *White Paper* issued in September 2016 by the International Swaps and Derivatives Association. It argues that blockchain holds great potential in the derivatives industry and advises to develop mechanisms to designate blockchain records as final as early in the transaction lifecycle as possible. International Swaps and Derivatives Association (ISDA), *The Future of Derivatives Processing and Market Infrastructure* (2016), available at <https://www2.isda.org/attachment/ODcwMA==/Infrastructure%20white%20paper.pdf> (last visited Oct. 27, 2016).

⁵⁰ As analyzed in the Allens Linklaters report referred in n. 16 above.

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.”⁵¹ A key question is to what extent, in addition to exchanging value, these systems are capable of exchanging property *in rem* rights.⁵² Exaggerated but conveniently imprecise claims are common. For instance, one of the authors of the Walport Report asserted that “unpermissioned 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*.”⁵³

In fact, however, even simple applications, such as bitcoin, require at least that intermediaries such as exchanges and “wallets” be used for the interface between the standard real world and the virtual world of digital currencies.⁵⁴ Such intermediaries have

⁵¹ David Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms* 1 (Coase-Sandor Inst. for L. & Econ. Working Paper 685, 2014), available at <http://www.law.uchicago.edu/files/file/685-dse-economic.pdf>.

⁵² Merrill & Smith, *supra* note 3; Hansmann & Kraakman, *supra* note 3.

⁵³ Simon Taylor, *Definitions*, in *DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN*, *supra* note 1, at 17.

⁵⁴ Even standard money is an abstraction: its value is determined by its ability to be used to acquire real assets. Digital money requires a similar but, for the time being, longer transformation. The importance of this interface 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 29, at 413.

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

often been insecure,⁵⁵ suffering frequent fraudulent attacks.⁵⁶ This presence of intermediaries is not necessarily bad. Even though, as blockchain partisans rightly point out, specialized enforcement and, in general, intermediation, entail agency costs, they enjoy the advantages of specialization: the economy is based on specialization.

In blockchain applications, these interfaces between the digital and the real worlds resemble the traditional interface between contractual (in personam) and property (in rem) rights. Contractual systems often require at least one intermediary (a registry or a court) between the world of mere claims or in personam rights and the real world of in rem rights. (With the exception of those purely based on possession.)⁵⁷ For example, in property 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.⁵⁸ Note that, in a sense, a

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 11, at 19. *See also* http://www.cuber.ee/en_US/ (visited October 17, 2016).

⁵⁵ For Bitcoin, the blockchain itself has been resilient but the exchanges and wallets have not: “Using hackerproof bitcoin requires going through intermediaries such as exchanges to convert realworld currency into cryptocash, and “wallets” to store it. These have proved anything but secure, which arguably defeats the purpose of bitcoin’s trustfree world.” *Blockchain: The next big thing. Or is it?*, *ECONOMIST*, May 9, 2015, available at <http://www.economist.com/news/special-report/21650295-or-it-next-big-thing> [hereinafter *Blockchain: The next big thing. Or is it?*].

⁵⁶ Izabella Kaminska, *Bitcoin Bitfinex Exchange Hacked: The Unanswered Questions*, *FIN. TIMES* (Aug. 4, 2016), <https://www.ft.com/content/1ea8baf8-5a11-11e6-8d05-4ea66292c32>. 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. It is possible that public ledger platforms are more efficient than other alternative.

David Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms*, abstract (Coase-Sandor Inst. for L. & Econ. Working Paper 685, 2014), available at <http://www.law.uchicago.edu/files/file/685-dse-economic.pdf>. A more 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. Or is it?*, *supra* note 55.

⁵⁷ *See, on this*, Benito Arruñada, *The Titling Role of Possession*, in *LAW AND ECONOMICS OF POSSESSION 207* (Yun-chien Chang ed., 2015) and, more generally, *LAW AND ECONOMICS OF POSSESSION* (Yun-chien Chang ed., 2015).

⁵⁸ A pioneer developer of applications for land registries, Factom, put it in this way:

chain of paper title deeds is also “virtual,” as it reflects mere claims;⁵⁹ 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.

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 looks similar to the transfer of ownership in real property, where the consent of rightholders is required to transfer in rem rights.⁶⁰ 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,⁶¹ but with records and an element of consent.)

Nevertheless, there are two fundamental differences between the two 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.

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 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), *available at* https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf?raw=true.

⁵⁹ The “chain” in “blockchain” comes about from the fact that each block is linked cryptographically to previous blocks. 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.

⁶⁰ Arruñada, *Property Enforcement*, *supra* note 44; ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6.

⁶¹ Andreessen, *supra* note 9.

These are serious concerns when it is claimed that “any type of asset can be transferred using the blockchain”.⁶² The legal effects of such transfers, at least, would be limited to the transferring parties.⁶³ Indeed, property rights are in the sphere of public ordering,⁶⁴ and pure “privacy” is only viable when parties trade in contractual claims.⁶⁵ As this has obvious welfare implications in terms of weaker enforcement,⁶⁶ 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.⁶⁷ 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.⁶⁸

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.⁶⁹

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 similar caveat is introduced by Abramowicz when he considers the limitations of bitcoin:

what makes Bitcoin remarkable is that it settles the most controversial issue—who owns wealth—without need for a law 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*

⁶² *The Great Chain of Being Sure about Things*, *supra* note 8, at 20.

⁶³ “Peer-to-peer law is most plausible as a mechanism of voluntary private ordering.” Abramowicz, *supra* note 29, at 365.

⁶⁴ Arruñada, *Property as Sequential Exchange*, *supra* note 4.

⁶⁵ Arruñada, *Coase and the Departure from Property*, *supra* note 4, and Arruñada, *Property as Sequential Exchange*, *supra* note 4.

⁶⁶ ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 18-24.

⁶⁷ Arruñada, *Coase and the Departure from Property*, *supra* note 4, at 305, and Arruñada, *Property as Sequential Exchange*, *supra* note 4.

⁶⁸ See note 49, above, on financial derivatives and section C, below, on the registration of legal organizations.

⁶⁹ Andreessen, *supra* note 9 (emphasis added) *The Great Chain of Being Sure about Things*, *supra* note 8.

*transfers of Bitcoins will be validated and added to a list of approved transfers, known as the block chain.*⁷⁰

Moreover, the meaning of “property rights” in the previous quotation is as in economics: 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. Insights from the theory of property rights

Different aspects of blockchain can be better understood from the theory of property, in rem, rights. First, the distinction between initial and recurrent allocation of rights, which is a requirement for in rem rights.⁷¹ Blockchain discussion and initiatives do not yet suffer 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.⁷² However, in this vein, one could imagine that, 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.

In contrast, blockchain applications follow the path of common efforts in property titling and administrative simplification in paying scant attention to legal rights,⁷³ 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

⁷⁰ Abramowicz, *supra* note 29, at 361 (emphasis added).

⁷¹ 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.

⁷² Arruñada, *Property as Sequential Exchange*, *supra* note 4.

⁷³ *Id.*

narrowly attribute to poor data management. E.g., “the 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.”⁷⁴ 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, making sure that transactions are not contradictory with preexisting property rights and do not create new collisions of claims.⁷⁵ Despite the fact that this is mainly a legal issue, not a technological issue, blockchain applications in property registration focus instead on archiving, 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,⁷⁶ claims on the potential of the technology in this area should be substantially diluted.⁷⁷

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 contract and when Lantmäteriet receives the bill of sale and make the approval of the title is often three to six months . . . [and] the issues above have resulted in sellers, buyers, banks and real estate agents being forced to create their own complex, red tape, processes for

⁷⁴ DOBHAL ABHISHEK & MATTHEW REGAN, IMMUTABILITY & AUDITABILITY: THE CRITICAL ELEMENTS IN PROPERTY RIGHTS REGISTRIES 3 (2016).

⁷⁵ 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)) comes close to assuming perfect information and seems, for the reason given in the text, inadequate.

⁷⁶ As seemingly recognized when asserting that “blockchain 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).

⁷⁷ This may help to explain why projects stall soon after big and seemingly exaggerated announcements: e.g., Honduras. Pete Rizzo, *Blockchain Land Title Project ‘Stalls’ in Honduras*, COIN DESK (Dec. 26, 2015), <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.*

agreements between them since they have to make sure that things can't go wrong, and because the value of the transactions is large.⁷⁸

However, all these three points deserve important qualifications:

First, it is not fully true that land registries are “involved in a few steps at the end of the real estate transactions” because they provide crucial information on possible conflicting claims from the beginning and during the whole contracting path. For instance, in step 3 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.”⁷⁹ Similar contacts are made in steps 10 and 21, 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,”⁸⁰ and further contacts are made by banks in connection with mortgages at steps 25 and 27.⁸¹ Moreover, there are costs and benefits associated with transparency. The tradeoff cannot always be assumed to be necessarily positive.

Second, the typical complaint that the systems are “slow at registering transactions” 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.,⁸² activities which 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.

⁷⁸ KEMPE, *supra* note 11, at 8-9.

⁷⁹ *Id.* at 23.

⁸⁰ *Id.* at 24.

⁸¹ *Id.* at 26.

⁸² *See, e.g., Id.* at 23-25.

V. ASSESSING BLOCKCHAIN APPLICATIONS IN PROPERTY

The above 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 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 role of legacy systems, and the limitations and opportunities in the areas of property conveyancing and deed recordation, as well as company and property registration.

For a start, a cautionary note is in order, as 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”.⁸⁴ Certainly, he immediately asserts that “the purpose of the replicated database is simply to *securely agree on who owns what*”,⁸⁵ and this “securely agree” is essential to move from in personam to in rem.

A. Private blockchains and “legacy” systems

First of all, it is worth considering that, for all types of assets, moving legacy systems into blockchain applications would suffer from two old enemies of institutional innovations: the conservatism of users, and the private interests of the professionals whose human capital is tied to the current systems. Both factors make it likely that, at least initially, applications will be limited to using the blockchain only for notarization and data archiving within “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.⁸⁶ In particular, private blockchains should expand rapidly to implement transactions in closely-knit networks of suppliers, manufacturers and distributors, which

⁸³ Nick Szabo, *Secure Property Titles with Owner Authority*, <http://szabo.best.vwh.net/securetitle.html>, at 1 (last visited Aug. 10, 2016).

⁸⁴ *Id.* at 2.

⁸⁵ *Id.* (emphasis added).

⁸⁶ On the comparative advantages of public and private blockchains, 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/>.

are already characterized by phenomena such as “contract manufacturing”,⁸⁷ as well as “virtual integration.”⁸⁸ Financial institutions are pioneers in this regard.⁸⁹ They face a basic contradiction, however: the smaller the network, the fewer the advantages of decentralization, and the easier it may be to manipulate it.

Prospects for blockchain are therefore better for assets that lack legacy systems: sophisticated solutions in intellectual property and new private registries for certain high-value assets, as in the Everledger initiative for registering diamonds and other specially valuable assets. 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.”⁹⁰ Here, therefore, blockchain seems to enjoy a particular

⁸⁷ Benito Arruñada & Xosé Henrique Vázquez, *When Your Contract Manufacturer Becomes Your Competitor*, 84 HARV. BUS. REV. 135 (2006). On the effects of blockchain on organizational structure, see, e.g., IBM INSTITUTE FOR BUSINESS VALUE, FAST FORWARD: RETHINKING ENTERPRISES, ECOSYSTEMS AND ECONOMIES WITH BLOCKCHAINS (2016), available at <http://www-935.ibm.com/services/us/gbs/thoughtleadership/blockchain/> (last visited Dec. 2, 2016).

⁸⁸ 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), <http://blogs.wsj.com/cio/2016/10/19/wal-mart-turns-to-blockchain-for-tracking-pork-in-china/>.

⁸⁹ 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), <http://www.wsj.com/articles/how-blockchain-will-change-your-life-1478564751>. “Having initially been sceptical about it 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 “allows organizations to rapidly design, deploy and operate distributed ledgers”, managed permissions, controlling “who can connect to your blockchain, send and receive transactions, create assets and blocks”. The chain is therefore “as open or as closed as you need” (<http://www.multichain.com/>, visited August 12, 2016). The big question on private blockchain is 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 and present even in vertically integrated structures due to agency problems.

⁹⁰ 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).

advantage if it is capable of relaxing this constraint, so that it becomes economically viable to identify each individual asset, one of the objectives of the Everledger registry.⁹¹

B. 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. In particular, they are defined by the fact that in all property systems parties are free to choose their lawyers, conveyancers and notaries public. 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.⁹² Therefore, blockchain should find it easier to expand into notarization and data archiving,⁹³ but will find it more difficult to replace land registries, especially in jurisdictions, such as Australia, England, Germany or Spain, that have registries of rights, also often called “land registration” or “title by registration” systems.⁹⁴

First, to the extent that even in civil law jurisdictions notaries public are freely chosen by parties to private contracts, the blockchain will play a bigger role in notarization. The only functions for which notaries used to be clearly superior were in identifying parties and, more clearly, in ascertaining their legal capacity.⁹⁵ However, both advantages are

⁹¹ Natasha Lomas, *Everledger Is Using Blockchain To Combat Fraud, Starting With Diamonds*, TECH CRUNCH (June 29, 2015) <https://techcrunch.com/2015/06/29/everledger/> (last visited Oct. 25, 2016). See also Leanne Kemp, *Case study – Diamonds*, in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, supra note 1, at 56.

⁹² Arruñada, *Property Enforcement*, supra note 44, at 424–28.

⁹³ 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.” Angela M. Sasse, *Security and Privacy*, in DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, supra note 1, at 47.

⁹⁴ For an analysis of the different types of land registries, see Arruñada, *Property Enforcement*, supra note 44, at 406–23.

⁹⁵ Benito Arruñada, *Market and Institutional Determinants in the Regulation of Conveyancers*, 23 EUR. J. L. & ECON. 93 (2007), who 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 under a principle of *numerus clausus*, 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).

also threatened by complementary technological developments in identification and the related availability of registries for individuals' legal capacity. Moreover, both functions are 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 you have the required permissions (authorization).⁹⁶

Second, the applicability of blockchain to registries will be more limited because they play a public legal function, protecting the interest of unrepresented third parties and therefore being much more than mere public databases.⁹⁷ Moreover, 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

⁹⁶ For a more nuanced analysis of the authentication and authorization requirements, specifically developed to compare legacy and electronic conveyancing and titling systems, see Rod Thomas, Rouhshi Low & Lynden Griggs, *Australasian Torrens Automation, Its Integrity, and the Three Proof Requirements*, 2013 N.Z. L. REV. 227 (2013) and *Designing an Automated Torrens System — Baseline Criteria, Risks and Possible Outcomes*, 2015 N.Z. L. REV. 425 (2015). See also, for an application to blockchain, Rod Thomas & Charlie Huang, *Blockchain, the Borg Collective and Digitalisation of Land Registries*, December, THE CONVEYANCER (Forthcoming Dec. 2016). The case of the Estonian government is particularly interesting:

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 *DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN*, supra note 1, at 83.

⁹⁷ 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, but 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 claims but the rights on a specific property. The "ledger" terminology focuses on the numeric or accounting aspect while the key element in registries is legal: they do not mainly contain magnitudes (values) but the legal evidence supporting claims (recording) or certifying rights (registration).

only to register and track property but to define new types of property rights, including multiple ownership and asset-sharing with sophisticated allocations of use rights.

In principle, when considering the impact of blockchain for property registries, it is sensible to 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. 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.⁹⁸

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 some public authority to establish the rules of evidence: to set the value of the blockchain as a source of evidence for in rem adjudication. To produce in rem effect, all parties must be obliged to express their will through the blockchain. Moreover, this authority must trust those designing, putting in place and—to some extent—governing, or at least affecting, the decentralized government of the blockchain system.

C. Company registration

The case of company registries is similar, to the extent that most of them are closer to recordation than to registration systems. However, company registries could be challenged by initiatives like the Ethereum blockchain as this aims 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.⁹⁹ A less ambitious initiative is that of developing an international standard for the identification of legal entities, known as the Register of Legal Organizations (ROLO).¹⁰⁰ It is revealing that, despite being led by collaborative industry, given that most transactions are business-to-business (B2B), what is being considered is the need for ROLO “in each nation”,¹⁰¹ and the expected presence of a mandatory element. In particular, “enrolling into a ROLO at a Level of Assurance is voluntary; however, being

⁹⁸ ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 55–67.

⁹⁹ Compare Abramowicz, who claims that “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.” Abramowicz, *supra* note 29, at 414.

¹⁰⁰ See ANDREW COAKLEY, THE BLOCK CHAIN NETWORK: ACCELERATING ADOPTION, 5 available at <http://www.slideshare.net/AndrewCoakley1/blockchain-final-25112015-v11>.

¹⁰¹ *Id.* at 5.

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”.¹⁰² In England, it has the support of Companies House, the English company register.¹⁰³

Another area related to company registration in which blockchain has the potential to automatize transactions is that 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, 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.¹⁰⁴ In both directions, blockchain could make the whole process much more efficient and automatic.¹⁰⁵

D. Property registration

In comparison with property recordation and company registries, property registries of rights (often called “title systems”) should be less affected by blockchain, to the extent that registration review cannot be easily exercised by an automatic system: they would be facing even greater difficulties than those considered above with respect to contractual completion. (All registries of rights 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 the system.)

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 2009,¹⁰⁶ but with a key difference: the Land Register would at least

¹⁰² *Id.* at 6.

¹⁰³ *Id.* at 6.

¹⁰⁴ On the considerable costs and risks, both actual and potential, of these systems, see the report sponsored by the US Depository Trust & Clearing Corporation and produced by OXERA, CORPORATE ACTION PROCESSING: WHAT ARE THE RISKS? (2004), available at <http://www.oxera.com/Oxera/media/Oxera/downloads/reports/Corporate-action-processing.pdf?ext=.pdf> (last accessed Oct. 16, 2016). It estimated at one million the number of corporate actions worldwide. It estimates the annual risk at between 1.6 and 8 billion Euros and annual actual losses at between 300 and 400 million Euros. *Id.* at i.

¹⁰⁵ See Dominik Hobson, *Case study – Corporate actions, in* DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN, *supra* note 1, at 58–59.

¹⁰⁶ The changes proposed in Sweden are summarized at KEMPE, *supra* note 11, at 27–31. See also, for implementation issues, ALEX MIZRAHI, A BLOCKCHAIN-BASED PROPERTY OWNERSHIP

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.”¹⁰⁷ Moreover, the land 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. In other words, Lantmäteriet guarantees which digital representation a specific property has.¹⁰⁸

Therefore, the only substantial differences proposed in the *White Paper* seem to be, on the one hand, the development of a blockchain application for electronic conveyancing, application which would make it possible for all parties involved to work with the same information, expanding their knowledge, and reducing duplications and

RECORDING SYSTEM (Chroma Way) (2016), available at <http://chromaway.com/papers/A-blockchain-based-property-registry.pdf> (last visited Oct. 27, 2016); as well as a graphical demo at <http://chromaway.com/landregistry/> (last visited Oct. 27, 2016). For a description and analysis of the New Zealand case, see Benito Arruñada, *Leaky Title Syndrome?*, *New Zealand Law Journal* 115 (2010), and, for a more general discussion of electronic conveyancing see ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 208–15.

¹⁰⁷ KEMPE, *supra* note 11, at 34. 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, 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. at 33. Moreover, “the land registry of Lantmäteriet is, in principle, entirely separate from the solution.” *Id.* at 34.

¹⁰⁸ *Id.* 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.

mistakes. This raises the previous question about the real costs and benefits of this simplification, including as a cost the potential for added rigidity associated with the possibility that a stricter numerus clausus may affect even the personal contractual stage. Perhaps more importantly, all parties would also have, through the application, instant access to any filing in the register that may affect the legal standing of the rights being traded.

On the other hand, the system is planned to work with “pending property titles” during the whole conveyancing 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 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.¹⁰⁹

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. In principle, it is unclear how they would be affected by the new system. If this 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.¹¹⁰ 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 be upgraded to “conditional” property titles.

VI. CONCLUDING REMARKS ON FIRMS, CONTRACTS AND PROPERTY

Blockchain is said to be “trustless”, pointing out that it does not need trust to work. However this trustless feature needs to be qualified. Blockchain and all other institutional and physical technologies supporting impersonal exchange 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. Blockchain enthusiasts claim that it gets rid of intermediaries but this claim proves illusory: it is more a Holy Grail than a realistic objective. The paper shows the major roles played by different types

¹⁰⁹ *Id.* at 22.

¹¹⁰ ARRUÑADA, INSTITUTIONAL FOUNDATIONS, *supra* note 6, at 210–12.

of intermediaries. Their presence holds consequences for firms' strategy and the structure of contracting:

First, blockchain applications will tend to rely on dual structures of causal and formal transactions, with the formal stage being highly abstract, using simple contracts and enforcing a closed number of property rights.

Second, the core peer-to-peer structure of blockchain faces insurmountable difficulties to reach contractual completion and to interact with the real world, 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.

Fourth, the emergence of specialized agents will reduce total 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.

More generally, because of the role of intermediaries, blockchain is likely to affect transaction costs in all types of transactions, modifying the comparative advantage 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 the sign of these impacts are open to question. Therefore, contrary to expectations, it is debatable if blockchain really favors market transactions over business firms.

Lastly, blockchain will find it easier to enable transactions in personal 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 property conveyancing, as well to, at most using private blockchains for archiving purposes within standard registration systems.