Cyberspace Law Institute and Winter Working Meeting
January 25-26, 2019
Stetson University School of Law
Gulfport, FL

Blockchain Technology --- It’s Not Just for Bitcoin Any More!

John Ottaviani, Partner, Partridge Snow & Hahn LLP, Providence, RI
Carla Reyes, Assistant Professor of Law & Director of Center for Law, Technology & Innovation, Michigan State Univ. College of Law, East Lansing, MI

This program will introduce the current state of actual novel use cases of blockchain technology and smart contracts and discuss the legal implications.
Blockchain Technology --- It’s Not Just for Bitcoin Any More!

TABLE OF CONTENTS

Presentation Slides .................................................................1
Abstract ..................................................................................xx
Bios ....................................................................................xx
Supplemental Materials ...........................................................xx

3410902.1/777778-76
Blockchain Technology – It’s Not Just for Bitcoin Any More!

ABA Cyberspace Law Committee Winter Working Meeting

John E. Ottaviani
Partner
Partridge Snow & Hahn LLP

Carla L. Reyes
Assistant Professor of Law & Director of the Center for Law, Technology & Innovation
Michigan State University College of Law

Faculty Associate
Berkman Klein Center for Internet & Society at Harvard University
Image Credit: Richard Gendal Brown, A Simple Model for Smart Contracts, 
https://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/
SMART CITIES

Smart Energy
- Smart Grid
  - Smart Grid asset mgt
  - Smart generation
  - Demand side mgt
  - Utility Services
- Microgrid
- District heating/cooling Mgt
- Gas Distribution Mgt
- Shore connection

Smart Mobility
- EV Charging
  - Infrastructure & Supervision Services
- Traffic Mgt
  - City Traffic
  - Highway Traffic
- Tunnel Management
- Tolling Management
- Railway Mgt
- Airport Solutions

Smart Water
- Plant & Network
  - Energy Performance
- Water Distribution
  - Optimization & Loss Mgt
- Stormwater Mgt
  - & Urban Flooding
- Irrigation Mgt

Smart Public Services
- Public Safety
  - Video Surveillance
- Smart Street
  - Street Lighting

Smart Building
- Multiple Disparate Building Mgt
- High-performance Buildings
- Smart Street
  - Street Lighting
- Efficient Homes

Smart Data Center
- Efficient Data Centers
- Prefabricated Date Centers
- Infrastructure
  - Mgt Enabled Services

Smart Collaboration
- Planning & Design
- Solution implementation
- Operation & Optimization
- Business models and financing

City-wide Platforms
- Energy & Sustainability Resource mgt
- Urban Efficiency Platform
- District Energy Mgt Information System

Cross domains application
- Weather
- Gis
- Asset mgt
Starting from birth, patients accumulate data from clinical encounters, wearable devices, etc., and each data upload adds a new block to their electronic health chain. Records of the types of data amassed (vaccination histories, pathology reports, etc.) are stored on the patient’s electronic health chain.
Legal agreements are marked-up using our domain specific markup-language, turning contracts into computable objects.

Evidence of “state” of agreement and electronic signatures are stored on the Ethereum blockchain.

Once signed, agreements trigger smart contracts in secure and private execution environment.

Public and private APIs allow third parties to integrate OpenLaw Protocol into their respective systems and build blockchain-based applications.

https://youtu.be/HPbgR4gG_4E - Tax Law Demo
CORPORATE SHARE REGISTRIES
ARTICLE 9 UCC-1 FILING SYSTEM
SOME INTERESTING LEGAL AND PRACTICAL ISSUES

• Is the blockchain (paperless) transaction legal and enforceable without affirmative authorization?

• Is blockchain the right technology for the transaction? Would distributed ledgers work better? Is proof of work needed in all circumstances?

• Are smart contract developers “liable” for the consequences of the technology (for example, aiding and abetting violations of federal securities laws)?

• What law(s) apply to the rights and obligations of the parties?
BLOCKCHAIN TECHNOLOGY --- IT’S NOT JUST FOR BITCOIN ANY MORE!

There has been much press and hype about the development and use of blockchain technology and so-called “smart contracts.” Moving beyond the basics, this program looks at some real world use cases and pilots using blockchain technology, distributed ledgers, and smart contracts, and explores some of the legal and practical issues they raise.

Blockchain technology is a type of a broader technology known as “distributed ledger technology” or “DLT”, which has the potential to change how banking, insurance, supply chain management, real estate, health care and other industries transact and operate. Much as existing laws and regulatory frameworks have been applied and stretched to reach Internet-based business models, today courts, legislatures, and regulators around the globe are confronting similar challenges presented by DLT. To counsel clients properly, business lawyers require a fundamental understanding of this technology, its promised benefits, the potential costs, and associated legal and business risks.

This program will explore selected real world use cases of blockchain and smart contracts. The speakers also will identify and summarize legal and practical issues raised by the use of blockchain technologies and smart contracts for developers, vendors, and business end users.
Presenters

John Ottaviani --- Partridge Snow & Hahn LLP

- John is Chair of the Intellectual Property & Technology Group for Partridge Snow & Hahn LLP, and is based in the firm’s Providence, RI, office. He concentrates his practice in representing businesses and their owners, in protecting and enforcing trademarks and copyrights, and in preparing and negotiating intellectual property licensing agreements. He regularly advises clients on trademark, copyright, domain name, and trade secret issues that arise in the physical world and on the Internet. He also works on the intellectual property aspects of business financing, acquisition and sale transactions. John also has extensive experience in preparing and negotiating agreements for technology companies and for companies using technology in all industries.

Carla Reyes --- Michigan State University College of Law, Berkman Klein Center for Internet and Society at Harvard University

- Carla Reyes is an Assistant Professor of Law and Director of the Center for Law, Technology & Innovation at Michigan State University College of Law, and a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. A former Fulbright Scholar, her current research focuses on the intersection of blockchain technology and the law, theorizing about the technology from a commercial and corporate law perspective. Professor Reyes also serves as the research director for the technology committee of the Uniform Law Commission, as a review editor for the Frontiers in Blockchain Journal section on Smart Contracts, and actively contributes to blockchain technology initiatives at the United Nations Internet Governance Forum, the American Bar Association, and the Coalition of Automated Legal Applications (“COALA”). Prior to joining the MSU Law College faculty, Professor Reyes taught business and commercial law courses at Stetson University College of Law as a Visiting Assistant Professor of Law from 2016-2018. Prior to law teaching, Professor Reyes practiced technology transactions law as an associate in the Blockchain Technology and Digital Currency industry group at Perkins Coie LLP.
More Legal Aspects of Smart Contract Applications

Token Sales, Capital Markets, Supply Chain Management, Government and Smart Cities, Real Estate Registries, and Enabling Self-Sovereign Identity
# Table of Contents

INTRODUCTION .............................................................................................................................................................................. 3

I. A (VERY) BRIEF INTRODUCTION TO SMART CONTRACTS .............................................................................................................. 3
   THE ORIGINS OF SMART CONTRACTS ............................................................................................................................ 3
   SMART CONTRACTS IN A DISTRIBUTED LEDGER TECHNOLOGY WORLD ........................................................................ 4

II. CURRENT ACADEMIC LITERATURE AND INDUSTRY INITIATIVES RELATING TO SMART CONTRACTS .......... 6
   SMART CONTRACTS AND CONTRACT LAW ............................................................................................................................ 6
   TECHNICAL DIFFICULTY POSED BY SMART CONTRACT DEVELOPMENT ........................................................................ 6
   INDUSTRY INITIATIVES RELATING TO LEGALLY ENFORCEABLE COMPUTATIONAL CONTRACTS .................................................. 7
   STATE LEGISLATIVE EFFORTS RELATED TO SMART CONTRACTS ...................................................................................... 8

III. EXPLORING THE LEGAL ASPECTS OF SMART CONTRACT APPLICATIONS ................................................................. 9
   SMART CONTRACTS IN TOKEN SALES .............................................................................................................................. 9
   SMART CONTRACTS IN CAPITAL MARKETS ................................................................................................................... 15
   SMART CONTRACTS FOR SUPPLY CHAIN MANAGEMENT ................................................................................................. 16
   SMART RECORDS FOR GOVERNMENT AND SMART CITIES ........................................................................................... 18
   SMART CONTRACTS FOR REAL ESTATE REGISTRIES ........................................................................................................... 20
   SMART CONTRACTS FOR ENABLING SELF-SOVEREIGN IDENTITY .................................................................................... 22

IV. AN INITIAL RISK MITIGATION CHECKLIST FOR BUSINESSES DEVELOPING SMART CONTRACTS APPLICATIONS ....... 24

V. CONCLUSION ........................................................................................................................................................................ 24
Introduction

Smart contracts have received significant attention from legal academics and attorneys for the impact they may have on contract law and the role of lawyers. Some have also identified and described a series of use cases for smart contracts. However, the literature currently lacks a comprehensive discussion of the legal implications of use cases that are unrelated to contract law. To fill that gap, in May 2017 we first published a white paper entitled “Legal Aspects of Smart Contract Applications,” which offered an initial analysis of the legal aspects of five prominent smart contract use cases. This updated edition of the white paper offers new analysis refined by the regulatory and industry activity undertaken since May 2017 through six use cases: token sales, capital markets, supply chain management, smart government records and smart cities, real estate land registries, and self-sovereign identity. We continue to maintain that legal risk is inherent in each of these subject areas, but with careful risk mitigation planning, companies can overcome many of those hurdles to offer effective products and services.

This updated white paper proceeds in four parts. Part I defines the terms blockchain and distributed ledger technology as used for the purposes of this white paper and then briefly surveys the relevant technological characteristics of smart contracts, the platforms upon which they operate, and the challenges that face those creating and executing them. In Part II we review the current literature from both leading industry groups and academia regarding smart contracts and acknowledge emerging industry efforts to build platforms for legally enforceable computational contracts. Part III introduces six uses of smart contracts in business and government processes, and examines the legal regime(s) applicable to each. Finally, in Part IV we offer insight into practical steps a business may take to mitigate legal risk when launching a product or service that uses smart contracts.

I. A (VERY) BRIEF INTRODUCTION TO SMART CONTRACTS

The term “smart contract” is widely used, and at times misused. For example, the term is frequently used when considering whether natural language contracts can be adequately translated into computer code, or whether computer programs can themselves represent a legally binding contract. Although interesting questions, these are not the primary issues in play for most smart contract implementations. To avoid adding to the definitional confusion that often plagues smart contract discussions, and to provide a common starting point for the rest of our analysis regarding the legal aspects of smart contract applications, this white paper begins by offering a brief introduction to smart contracts.

THE ORIGINS OF SMART CONTRACTS

The idea of smart contracts originated as early as 1994 when Nick Szabo first coined the term, using it to refer to “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.” Szabo’s original idea of smart contracts was broad enough that some smart contracts will fulfill the requirements of a legally enforceable contract while others will not. Szabo’s idea lay dormant for many years because the technology did not yet exist to support the implementation of smart contracts. Then, in 2009, the Bitcoin blockchain emerged—itself a limited form of a smart contract. Later, Ethereum offered an enhanced ability to build more complex smart contracts by using a specific smart contract language (Solidity) to enable developers to write complex processes in a short span of code. The rise of these protocols led to the resurgence of the smart contract idea and its increasing popularity as a tool for enhancing business processes and efficiencies. Integrating Szabo’s original idea into the new technological age of blockchains, however, has proved more difficult than perhaps initially anticipated.

---

2 Szabo’s original idea of smart contracts was broad enough that some smart contracts will fulfill the requirements of a legally enforceable contract while others will not.
3 Then, in 2009, the Bitcoin blockchain emerged—itself a limited form of a smart contract.
4 The rise of these protocols led to the resurgence of the smart contract idea and its increasing popularity as a tool for enhancing business processes and efficiencies. Integrating Szabo’s original idea into the new technological age of blockchains, however, has proved more difficult than perhaps initially anticipated.
SMART CONTRACTS IN A DISTRIBUTED LEDGER TECHNOLOGY WORLD

The Bitcoin blockchain, Ethereum, and other similar software protocols—which we refer to generally in this white paper as distributed ledger technology (“DLT”)—reignited the viability and usefulness of smart contracts. We use the term “DLT” broadly to refer to “computer software that is distributed, runs on peer-to-peer networks, and offers a transparent, verifiable, tamper-resistant transaction-management system maintained through a consensus mechanism rather than by a trusted third-party intermediary that guarantees execution.” We recognize that there exists a vivid debate about the appropriate use of the terms “blockchain” and “DLT” to describe various applications in the industry. We do not intend to engage in that debate here, nor does our adoption of the term “DLT” in this white paper reflect a position on that debate. Rather, we use the term “DLT” with the intention that it broadly encompass various forms of decentralized and distributed technology that have relevance to smart contract applications. The term “DLT” is increasingly used in academic literature and among standard-setting bodies as the broadest term, covering the Bitcoin blockchain, the Ripple protocol, Ethereum, and others. Further, DLT is broad enough to capture emerging platforms such as R3’s Corda. DLT also encompasses both proprietary (permissioned) DLT and open source (permissionless). DLT. For the purposes of this white paper, using the broadest possible term allows us to convey the important reality that the legal issues discussed here are equally applicable to smart contract applications built on any blockchain protocol or platform.

In the world of DLT, a smart contract is “a computer protocol—an algorithm—that can self-execute, self-enforce, self-verify and self-constrain the performance of its instructions.” So conceived, it is clear that smart contracts are not the same as blockchain applications; rather, “smart contracts are usually part of a decentralized (blockchain) application.” The Bitcoin blockchain itself is a smart contract with the limited purpose of executing transactions that involve the exchange of assets. However, DLT also enables smart contracts that go beyond simple funds transfers by embedding more extensive instructions into their computer code. In fact, some DLT protocols are specifically designed to enhance the ability of software developers to build applications that rely on more complex smart contracts. For example, Ethereum, with its smart contract-specific programming language Solidity, “allows you to program the future, to implement rules governing the array of possibilities that fan out from the present.”

---

7 Reyes, supra note 3, at 390-91 (citations omitted).
9 “Permissioned DLT” is used here to refer to DLT that is developed and used on a proprietary basis, and that is often not public. Angela Walch, The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, 18 NYU J. LEGIS. & PUB. POL’Y 837, 840-41 n.15 (2015).
10 “Permissionless DLT” is used here to refer to open source DLT—generally public ledgers, open for anyone to inspect. Id.
11 We also recognize that an ongoing debate exists regarding the terms “distributed” as opposed to “decentralized,” and “transparent” as opposed to “public.” Again, we adopt “distributed” and “transparent” for the purposes of this white paper without any intention to engage in or state a position in that debate. For the purposes of our legal analysis, it is useful to recognize that even when DLT is permissioned, it is possible to give certain outsiders (e.g., regulators) keys to the protocol for the purpose of inspection and audit. As such, permissioned DLT remains transparent, even if it is not public in the same way as permissionless DLT. Similarly, although we are aware that many object to the basic premise of permissioned DLT insofar as the concept necessarily means the protocol is not as decentralized as the permissionless origins, we use “distributed” as opposed to “decentralized” because permissioned DLT exists and is in use. As a result, the legal discussion in this white paper must consider both forms of DLT; otherwise, our analysis would only partially address the current landscape of the technology and the law. For further discussion and rationale on the definitional choices made here, see Reyes, supra note 3, at 390-91 n.29.
14 Mougayar, supra note 4.
15 Brown, supra note 5.
16 Henning Diedrich, Ethereum 67 (2017), “Ethereum has its focus on smart contracts instead of on being exclusively a digital currency. And as part of that, Ethereum transactions can be way more sophisticated than Bitcoin’s: full-fledged, high language programs, some many thousand lines long, which can call on each other, almost ad infinitum.” Id. at 39.
More specifically, “[a] smart-contract is an event-driven program, with state, which runs on a replicated, shared ledger and which can take custody over assets on that ledger.” This definition can be broken down into smaller parts as follows:

- Smart contracts are software programs that run on certain DLT protocols;
- Smart contracts are usually part of an application running on DLT, rather than standing alone as a DLT application;
- Smart contracts offer event-driven functionality—when triggered by external data (which may or may not require human input), smart contracts will modify other data;
- External data can be supplied by “oracles”—trusted data sources that send information to smart contracts (but not all smart contracts rely on oracles);
- Smart contracts can, acting on information provided by oracles, “enforce a functional implementation of a particular requirement, and can show proof that certain conditions were met or not met”;18
- Smart contracts can track changes in “state” over time;19
- Smart contracts are not the same thing as Ricardian contracts, which are digitized versions of natural language contracts that are linked to an automated function;20
- Smart contracts are autonomous in that the software developer who created them need not actively maintain, monitor, or even be in contact with them while they operate;21
- Once executed, smart contracts may be self-sufficient, in that they can be programmed to “marshal resources—that is, raising funds by providing services or issuing equity, and spending them on needed resources, such as processing power or storage;”22
- Smart contracts are distributed because they exist as software running on a DLT protocol that itself is distributed across a variety of network nodes;23 and
- Smart contracts guarantee execution of the contemplated transaction once the required conditions are met.24

Clearly, smart contracts offer the capacity to revolutionize any number of traditional processes, and as technologists and businesses craft new and existing uses of this technology, the law will struggle to keep pace. Our aim in this white paper is to provide an initial consideration of several smart contract application uses under current legal regimes. We also offer reflections and predictions on which legal issues and questions will be most important for smart contract applications moving forward. We begin our investigation of the legal aspects of smart contracts with a review of the currently available literature and current initiatives from academics and legal professionals regarding smart contracts.

17 Brown, supra note 5.
18 Mougayar, supra note 4. Ricardian contracts are “semantic representations that can track the liability of an actual agreement between parties.” For example, a Ricardian contract might represent the legal conditions of a digitized bond. Id (citing Ian Grigg, The Ricardian Contract (2004), http://ianq.org/papers/ricardian_contract.html.
19 DIEDRICH, supra note 16, at 20. “State” refers to “all or part of the data that a program deals with.” Id. Computer code that remembers things, then, is “stateful” computer code. DLT in general, and Ethereum in particular, is for stateful applications. As Vitalik Buterin explains, “[a]ll blockchains have a notion of a history—the set of all previous transactions and blocks and the order in which they took place—and the state—currently relevant data that determines whether or not a given transaction is valid and what the state after processing a transaction will be. Blockchain protocols also have a notion of a state transition rule: given what the state was before and given a particular transaction, (i) is the transaction valid, and (ii) what will the state be after the transaction?” Vitalik Buterin, Ethereum: Platform Review, Opportunities and Challenges for Private and Consortium Blockchains 1 (2015), https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cb/t/57506f387da24ff4f6ebc3c1/146489147417/Ethereum_Paper.pdf.
20 Mougayar, supra note 4.
21 Id.
22 Id.
23 Id.
24 DIEDRICH, supra note 16.
II. CURRENT ACADEMIC LITERATURE AND INDUSTRY INITIATIVES RELATING TO SMART CONTRACTS

To date, most of the discussion regarding smart contracts among attorneys and academics centers on contract law. Because of its prominence in the marketplace and the literature, we review that discussion here. We also review prominent literature regarding the difficulty of safely implementing smart contracts. Since we published the first version of this white paper, a number of industry initiatives relating to platforms for creating legally enforceable computational contracts have emerged. As any discussion of the current literature would be incomplete without a review of those efforts, we include a summary discussion of a few of those initiatives here. We also review the ongoing efforts in many states to adopt legislation relating to the legal enforceability of smart contracts. Finally, we highlight the differences between the contract law discussion and the legal aspects of smart contract applications that emerging use cases will confront in the near term.

SMART CONTRACTS AND CONTRACT LAW

Much of the current legal analysis of smart contracts centers on contract law. Such analysis focuses on smart contracts in a narrower sense than described above, focusing on “the use of computer code to articulate, verify and execute an agreement between parties.” Under a contract law analysis, key legal issues include notice, consent, and consumer protection—similar to the oft-litigated issues in the click-wrap and browse-wrap context. Others consider challenges under traditional concepts of fraud, force majeure and frustration. Still others view smart contracts, when used to automate the execution of a legal agreement, as merely a new form of self-help that fits rather neatly within existing contract law. Finally, several commentators consider the possible conflict between smart contracts and relational contract theory. Essentially, these authors recognize that a smart contract is merely a type of computer code, which may represent all, part, or none of a valid legal contract under U.S. law. Thus, even where a smart contract represents the entirety of an enforceable legal contract (often referred to as a “smart legal contract”), it remains subject to the same body of contract law as any other contract written in natural language.

As a result, most of the literature concludes that traditional contract law will continue to apply in a smart contract era, and that “smart contracts will never fully replace natural-language law.” Nonetheless, many authors also predict that smart contracts can bring clarity, predictability, auditability, and ease of enforcement to contractual relations. While the analysis of smart contracts as varying forms of legal contracts offers both useful and productive insights into the changing legal landscape, many of the current use cases for smart contracts involve proprietary platforms offered in the manner of software as a service, and do not purport to serve as a proxy for a traditional legal contract. This white paper offers an overview of the additional legal regimes that will bear upon such service offerings.

TECHNICAL DIFFICULTY POSED BY SMART CONTRACT DEVELOPMENT

A second set of literature involves substantial research demonstrating the challenges in correctly coding smart contracts to perform as intended, which can often be more difficult than programming traditional software. Furthermore, the self-executing nature of smart contracts causes even small errors to have significant consequences.

For example, the Ethereum-based decentralized autonomous organization, commonly referred to as “The DAO,” operated pursuant to a contract law analysis, key legal issues include notice, consent, and consumer protection—similar to the oft-litigated issues in the click-wrap and browse-wrap context. Others consider challenges under traditional concepts of fraud, force majeure and frustration. Still others view smart contracts, when used to automate the execution of a legal agreement, as merely a new form of self-help that fits rather neatly within existing contract law. Finally, several commentators consider the possible conflict between smart contracts and relational contract theory. Essentially, these authors recognize that a smart contract is merely a type of computer code, which may represent all, part, or none of a valid legal contract under U.S. law. Thus, even where a smart contract represents the entirety of an enforceable legal contract (often referred to as a “smart legal contract”), it remains subject to the same body of contract law as any other contract written in natural language.

As a result, most of the literature concludes that traditional contract law will continue to apply in a smart contract era, and that “smart contracts will never fully replace natural-language law.” Nonetheless, many authors also predict that smart contracts can bring clarity, predictability, auditability, and ease of enforcement to contractual relations. While the analysis of smart contracts as varying forms of legal contracts offers both useful and productive insights into the changing legal landscape, many of the current use cases for smart contracts involve proprietary platforms offered in the manner of software as a service, and do not purport to serve as a proxy for a traditional legal contract. This white paper offers an overview of the additional legal regimes that will bear upon such service offerings.

TECHNICAL DIFFICULTY POSED BY SMART CONTRACT DEVELOPMENT

A second set of literature involves substantial research demonstrating the challenges in correctly coding smart contracts to perform as intended, which can often be more difficult than programming traditional software. Furthermore, the self-executing nature of smart contracts causes even small errors to have significant consequences.

For example, the Ethereum-based decentralized autonomous organization, commonly referred to as “The DAO,” operated pursuant to a smart contract computer code. The code contained a known bug (that programmers were actively working to fix), which ultimately allowed
of The DAO's participants to divert 3.6 million ether ("ETH"), roughly valued at $50 million, into a “child DAO” controlled only by that participant. The DAO programmer, Christoph Jentzsch, was considered an Ethereum veteran at the time, demonstrating that even experienced programmers with a deep understanding of Ethereum can make mistakes when programming with smart contracts. In fact, because of the difficulty of coding smart contracts, leaders in the industry are advancing efforts to develop standard smart contract code audits. The point here is that, in addition to any other substantive legal issues triggered by the particular smart contract use case, businesses offering smart contract-based services should remain mindful of potential legal liability arising from programming mistakes, which may include product liability, breach of (the software as a service) contract, unfair and deceptive trade practices, and cybersecurity, among others.

INDUSTRY INITIATIVES RELATING TO LEGALLY ENFORCEABLE COMPUTATIONAL CONTRACTS

Despite the difficulty of programming smart contracts, academics and industry actors alike continue to see potential value in melding enforceable legal contracts with smart contract computer code. To realize this potential, and in light of the technical difficulty in making smart legal contracts commercially viable, several industry initiatives emerged to pursue platforms and standards to facilitate their broader adoption. We introduce several such initiatives here.

THE ACCORD PROJECT. Led by legal-technology startup Clause, the Accord Project is a consortium of technology and legal experts focused on developing the Accord Protocol—a series of legal and technical standards for developing and implementing smart legal contracts across multiple platforms. The project seeks “to integrate computable functionality into legally-enforceable contracts, while drawing upon a range of experts to establish an industry-first set of standards for the inevitable transition to computable contracting.” The Accord Project spearheads the development of an open source implementation of the Accord Protocol called “Cicero,” which offers a smart contract template system that enables the transformation of legally enforceable natural language agreements into smart legal contracts by connecting them “to a wide variety of software systems and platforms, including blockchain and enabling execution “in response to external data.”

OPENLAW. OpenLaw seeks to create “a technology stack to help power next generation ‘smart’ legal agreements.” More specifically, OpenLaw offers a “blockchain-based protocol for the creation and execution of legal agreements” that interacts with blockchain-based smart contracts, allowing the legal community to “more efficiently engage in transactional work and digitally sign and store legal agreements in a highly secure manner.” OpenLaw has developed a repository of legal agreement templates that can be modified using OpenLaw’s “Legal Markup” language to “create and manage the execution of legal documents, and, if desired, embed Ethereum-based smart contracts into legal agreements.” OpenLaw is also working to enable contract negotiation between OpenLaw users via the Ethereum blockchain, and integration with Stripe payments to facilitate payouts in fiat currency.

STANFORD COMPUTABLE CONTRACTS INITIATIVE. A third initiative comes from Stanford University. In connection with the broader work related to legal analytics and computational law at Stanford’s CodeX, the Stanford Computable Contracts Initiative works “on legal technology that will help move the world from natural language based contracts toward a world of computable contracts.” With the dual aims of reducing legal transaction costs and enabling better contracts, the Computable Contracts Initiative “works on developing a Universal Contract Definition Language that will allow terms and conditions to be represented in [a] machine-understandable way.” The Contract Definition Language aims to provide a uniform expression of contractual and legal terms in the form of executable computer code that can be employed across legal domains, with the goal of facilitating more efficient and optimal decision-making.

---

35 Id.
36 Diedrich, supra note 16, at 54.
42 Making Legal Contracts Smart, supra note 40.
43 Introducing OpenLaw, Medium (July 25, 2017), https://medium.com/consenSys-introducing-openlaw-73e4a1038b; see also OpenLaw, supra note 42.
44 Introducing OpenLaw, supra note 43.
49 Id.
STATE LEGISLATIVE EFFORTS RELATED TO SMART CONTRACTS

A variety of state legislatures have introduced legislation that purports to clarify that contracts cannot be denied legal effect, validity or enforceability merely because the contract is processed, executed, or otherwise enforced via smart contract computer code. States that have enacted, are considering, or have considered such laws include Arizona, 50 California, 51 Florida, 52 Nebraska, 53 Nevada, 54 and New York, 55 among others. Some of these statutes contain definitions of terms such as “blockchain,” “distributed ledger technology” and “smart contracts” that have come under significant fire by academics. 56 For example, the Arizona statute, signed into law in 2017, defines “blockchain technology” as “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless.” 57 The definition also provides that “[t]he data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth.” 58 One critique of such definitions centers on the use of terms, such as immutable, without accounting for the technical limitations of the technology. 59

Irrespective of the relative accuracy of the definitions contained in such laws, it is not at all clear that such legislation is necessary to render smart contracts legally enforceable. As discussed above, the leading academic scholarship in this area concludes that contracts processed, executed, or otherwise enforced via smart contract technology remain subject to existing contract laws, just like any other technologically enhanced contracts. Among the laws that apply are the federal Electronic Signatures in Global and National Commerce Act (“ESIGN Act”) 60 and the Uniform Electronic Transactions Act (“UETA”), which nearly all states have enacted. 61 The ESIGN Act and the UETA ensure that: if a law requires a signature, an electronic signature suffices; and if a law requires a record to be in writing, an electronic record suffices. A contract, signature, or related record may not be deemed unenforceable or to be without legal effect merely because it is in electronic form; and the use of an electronic record in the formation of the contract is insufficient, standing alone, to deny legal effect to the contract. Cryptographic signatures fit the definition of “electronic signature” contained in the ESIGN Act and the UETA. As a result, it is not at all clear that a new legal framework is required to ensure the validity or enforceability of signatures, records, or contracts that use smart contracts. Instead, commentators worry that the types of legislation currently under consideration are not only unnecessary, but may serve to create confusion rather than clarity.

EMERGING USE CASES TOUCH ON ENTIRELY DIFFERENT LEGAL REGIMES

With this existing landscape of legal and computer science research in mind, this white paper uses as its starting point reports of developing smart contracts use cases. In the subsequent section, we offer an overview of six such use cases, explain how smart contracts make them possible, and provide an introductory discussion of the applicable legal regimes.

56 See, e.g., Angela Walsh, The Path of Blockchain Lexicon (and the Law), 36 Rev. Banking & Fin. L. 713, 734, 743-45 (2017) (critiquing the use of fluid blockchain terminology in legislation and regulation, arguing, among other things, that “a diverging terminology can lead to inconsistent regulation across jurisdictions or subject matter areas, due to different ways of talking about (and potentially different understandings of) the technology, rather than differing underlying policy choices by regulators,” and criticizing the February 2017 Arizona law defining signatures “secured through a blockchain” as “electronic signatures” for its definition of the term “blockchain technology”).
57 Id. at 743-44 (quoting H.B. 2417, 53rd Leg., 1st Reg. Sess. (Ariz. 2017)).
58 Id. at 744 (quoting H.B. 2417, 53rd Leg., 1st Reg. Sess. (Ariz. 2017)).
59 Id. at 744-45.
61 The states that have not enacted the UETA include New York, Washington, and Illinois, and each of those states have adopted alternative statutes which give legal effect to electronic contracts and signatures.
III. EXPLORING THE LEGAL ASPECTS OF SMART CONTRACT APPLICATIONS

This section explores six emerging uses of smart contracts: token sales, capital markets, supply chain management, smart government records and smart cities, real estate registries, and self-sovereign identity. We first provide the context that led to the application of smart contracts in each area. We then offer a brief discussion of potential legal issues that may arise as projects in each area become more prominent and more frequent.

SMART CONTRACTS IN TOKEN SALES

How Are Smart Contracts Used in Token Sales?

The uses of smart contract applications in token sales that feature most prominently in the existing news cycle and regulatory debates include sales of tokenized goods and services, crowd sales, venture capital fundraising, and tokenized securities. However, a growing number of projects use smart contracts to create new offerings that operate more like a layered protocol than a decentralized application. In this section, we offer a short discussion of both token sales involving tokenized goods and services, and token sales involving this emerging class of protocol, governance, and autonomous tokens. The differences between types of tokens may have implications for the applicability of existing law to any given token sale.

DLT protocols, including the Bitcoin and Ethereum blockchains, represent what many refer to as “cryptoeconomic protocols” that rely on intrinsic tokens (e.g., bitcoin and ether, respectively) to encourage users to validate transactions, impose minor transaction costs to prevent spam without discouraging legitimate activity, and grant the token holder the right to participate in the network. The industry increasingly refers to tokens intrinsic to DLT protocols, such as bitcoin and ether, as “protocol tokens.” These intrinsic protocol tokens, sometimes referred to as tokens for native protocols, are far from the only type of token operating in the cryptocurrency ecosystem.

For example, smart contracts enable non-intrinsic tokens to exist on top of blockchains. Many recent token sales involve tokens that adhere to an Ethereum-based standard known as “ERC20.” Tokens designed in accordance with the ERC20 token standard (referred to as “ERC20 tokens”) are not intrinsic to the Ethereum blockchain, but are compatible with an Ethereum wallet and can readily implement other Ethereum token smart contracts. Although most tokens are built with the ERC20 token standard, the uses and purposes of ERC20 tokens vary significantly. For example, an ERC20 token may represent fungible goods, such as coins, gold certificates, loyalty points, IOUs, or in-app credits. Or, an ERC20 token may represent a tokenized right to a good or service within a decentralized application. When application tokens represent a tokenized good or service, they are increasingly referred to as “utility tokens.” Brave Browser’s Basic Attention Token (“BAT”) represents an example of a utility token. Brave Browser users earn BAT for watching advertisements, and can use earned BAT to access premium content.

---

61 In this context, the term “protocol” refers to “the set of cryptoeconomic rules that maintain distributed consensus across a peer-to-peer network.” Will Warren, The Difference Between App Coins and Protocol Tokens, MEDIUM (Feb. 1, 2017), https://blog.0xproject.com/the-difference-between-app-coins-and-protocol-tokens-7281a42b348c. Such cryptoeconomic protocols can be distinguished from the more general “network protocol,” which simply sets the rules that allow networked computers (nodes) to communicate with each other. Id. For example, the Internet Protocol is a network protocol that defines the digital message formats and rules for communication among connected computers. Internet Protocol (IP), TECHNOPEDIA, https://www.techopedia.com/definition/5366/internet-protocol-ip (last visited Mar. 29, 2018). Email is also built on a protocol that allows users to communicate with one another: “It’s just a way for two computers to talk to one another.” Ryan Shea, When to Use Protocol Tokens, MEDIUM (Nov. 13, 2017), https://medium.com/@ryanshea/protocol-tokens-1ed44a1a8453.


63 Id. at 14.

64 Warren, supra note 62.

65 Rohr & Wright, supra note 63, at 21.

66 The technical functions associated with the ERC20 Token Standard appear at: https://etherscan.io/erc2o-token-standard.

67 This list of tokenized goods appears at: https://www.ethereum.org/tokens, and is not meant to be exhaustive.

68 Such “application tokens” or “app tokens,” are defined as “tokens that are native to decentralized applications and have a cryptographic asset associated with their use or monetization, without locking value in its parent protocol.” Rafael Delfin, A General Taxonomy for Cryptographic Assets, Brave New Coin (2018), https://bravenewcoin.com/general-taxonomy-for-cryptographic-assets.

69 Rohr & Wright, supra note 63, at 22 (defining “utility tokens” as app tokens that “grant holders the right to access, use, and enjoy a given technology or participate in an online organization”).

70 Id. at 23. BAT would fall within the definition of application token in the Brave New Coin General Taxonomy. See Delfin, supra note 69, at 18 (including tokens for digital advertising in the category of application tokens).

71 Rohr & Wright, supra note 63, at 23. Other examples of application tokens offered by the Brave New Coin General Taxonomy include DigiDAO, CoEval, APX Ventures, Civic, Aragon, and AdEx. See, Delfin, supra note 69, at 17.
Increasingly, a new class of tokens is emerging in the ecosystem—namely, tokens that operate as a form of layered protocol token, built on top of a native cryptoeconomic protocol like Ethereum, that are imbued with governance attributes or sold in an entirely autonomous manner. At least one commentator refers to such protocols as “‘non-native’ cryptoeconomic and network protocols.” The 0x protocol is an example of a non-native network protocol, operating through a system of smart contracts on top of the Ethereum native cryptoeconomic protocol, that is designed explicitly for the decentralized exchange of tokens using publicly accessible smart contracts. The 0x protocol is entirely open source, and is maintained in part by proceeds earned in a public token sale of the 0x protocol token—ZRX. Holders of ZRX are granted governance rights concerning ongoing maintenance and updates to the 0x protocol. In addition, participants in the 0x ecosystem may choose to adopt ZRX for payment of transaction fees and other services offered within a proprietary platform.

Another example of a smart contract-based token that is markedly different from the ERC20 application tokens, utility tokens and capital raising tokens that have received so much recent attention include Metronome, a cross-chain monetary system oper ated entirely through autonomous smart contracts. The discussion of the legal issues relating to token sales described below focuses heavily on the types of tokens currently garnering the most regulatory attention: ERC20 tokens used to raise capital, including application tokens and utility tokens. The application of the laws discussed below to new and emerging types of protocol and autonomous tokens represents a further layer of regulatory complexity that merits careful attention and further industry and academic research.

**Legal Aspects of Using Smart Contracts in Token Sales**

Given the recent prominence of tokens and token sales, the legal issues that are currently at the forefront and which will continue to arise most frequently in the near term involve analysis as to the legal nature of a smart contract-based token and whether a token sale constitutes an offering of securities, a commodities contract, or some other regulated financial transaction. Depending on the legal nature of the token, particularly in the context of a crowd sale, the resulting tax consequences may also present novel issues for those interested in buying or selling tokens.

Although token sales are often intended to create ecosystems for accessing services through the tokens, the sales pose a significant risk of offering a security for sale and selling securities without proper authorization. If a token sale represents offering a security for sale, Section 5 of the Securities Act of 1933 generally requires that all securities offered for sale be registered with the Securities and Exchange Commission (“SEC”) unless an exemption applies. The federal securities laws define the term “security” very broadly to cover virtually all types of commercial financial instruments. What is covered by this definition can be vague in certain contexts, and thus the U.S. Supreme Court has developed a number of tests to determine whether a particular instrument is a security. Of such tests, the Supreme Court has made clear that the Howey investment contract test is applicable to cases involving “unusual instruments not easily characterized as ‘securities.’” The factors for the Howey test involve (i) an investment of money, (ii) in a common enterprise, (iii) with an expectation of profits, (iv) derived solely from the efforts of others. Howey is very dependent upon specific facts, however; depending on the circumstances of their issuance and the expectations of the parties, token sales could potentially be construed as “investment contracts,” and thus securities, under the federal securities laws. In fact, the SEC used the Howey investment contract test to determine that the tokens issued by the decentralized venture capital firm “The DAO” constituted securities.

---

**Notes:**

2. Will Warren & Amir Bandeali, 0x: An Open Protocol for Decentralized Exchange on the Ethereum Blockchain 11 (Feb. 21, 2017), https://www.0xproject.com/pdfs/0x_white_paper.pdf ("While 0x is fundamentally a network protocol used to facilitate signaling between buyers and sellers (rather than a cryptoeconomic protocol), it is intended to serve as an open standard for dApps that incorporate exchange functionality.").
3. Blake Henderson, Welcome to the 0x Community, Medium (Aug. 8, 2018), https://blog.0xproject.com/welcome-to-the-0x-community-9d999fe0e52b.
5. Id.
Although many industry actors seemed surprised by the SEC’s position, consideration of the specific elements of the Howey test reveals just how easily a token sale could fall into the investment contract category. For many token sales, the “investment of money” and “common enterprise” prongs are satisfied, because to purchase a token you make an investment of money, and the result of your investment is correlated to the results of other investors (i.e., token holders) or to the expertise of the token issuer. As a result, the “expectation of profits” and “solely from the efforts of others” elements of the test are often pivotal in determining whether a token sale constitutes an investment contract under federal securities laws. For an expectation of profits to exist, “the purchaser’s motivation in participating in the transaction must be securing a financial return.” When the purchaser buys the item for the purpose of consuming or using it, case law indicates that the transaction may not be treated as a security. The requirement that the expectation of profits be for profits generated by the efforts of others requires a similarly fact-dependent inquiry. Because the Howey test and, in particular, its “expectation of profits” prong, is so fact dependent, the outcome for any given token sale may be different, but that outcome will influence whether a token issuer ought to register with the SEC or else avail itself of an appropriate exemption before offering the token for public sale.

Recent SEC token sale enforcement activity prominently features the facts-and-circumstances nature of this analysis. For example, the SEC’s move to freeze the assets of both PlexCorps and RECoin rested on false promises of a thirteen-fold profit in less than one month and false disclosures regarding the nature of operations and the team consulting on the project. That the SEC took action against those that allegedly lied to investors is unsurprising.

A third enforcement action, however, offers additional insight into the multi-faceted nature of the fact-dependent inquiry undertaken by the SEC with regard to digital token sales. On December 11, 2017, the SEC announced that Munchee Inc. (“Munchee”) halted its token sale and refunded all token purchases after the SEC raised securities regulatory concerns. Munchee intended its token, MUN, to be a utility token, a token to incentivize honest and helpful reviews of restaurants through the pre-existing Munchee mobile app. Munchee’s white paper even acknowledged the Howey test and offered the utility token rationale as to why the MUN token did “not pose a significant risk of implicating federal securities laws.” In the enforcement order issued on December 11, 2017 (“the Munchee Order”), however, the SEC nevertheless unequivocally determined that “MUN tokens were securities pursuant to Section 2(a)(1) of the Securities Act. MUN tokens are ‘investment contracts’ under SEC v. W.J. Howey Co., 328 U.S. 293 (1946), and its progeny, including the cases discussed by the Commission” in the SEC DAO Report. The Munchee Order found that MUN token purchasers would have had a reasonable expectation of receiving future profits from the efforts of others through the revision of the Munchee mobile app and Munchee’s creation of an ecosystem for use of the tokens. The SEC specifically noted that at the launch of its ICO efforts, Munchee announced, among other things, “the way in which MUN tokens would increase in value, and the ability for MUN token holders to trade MUN tokens on secondary markets.” The SEC further noted that although MUN token purchasers were promised the ability to use MUN tokens to buy goods and services through the Munchee app in the future, no such functionality was available at the time of the token sale. Further, the Munchee Order focused on Munchee’s description of building an ecosystem and the resulting increase in value of MUN tokens that would allegedly result. Other important factors included Munchee’s marketing statements indicating that the company expected MUN tokens to rise in value and the ways in which Munchee would work to ensure as much, including arranging for MUN tokens to be traded on secondary markets.
Taken together, the SEC determined that, despite an apparent use for MUN tokens in the future, MUN token purchasers had a reasonable expectation of profits from the efforts of Munchee, making the MUN tokens an investment contract under Howey, and thus a security.\textsuperscript{98} Particularly noteworthy for future token sales, the SEC explained that “[e]ven if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labeling—such as characterizing an ICO as involving a ‘utility token’—but instead requires an assessment of ‘the economic realities underlying a transaction.’ All of the relevant facts and circumstances are considered in making that determination.”\textsuperscript{99} All told, those considering the launch of a token sale should consult legal counsel at every step of the sale in order to minimize regulatory risk, as the analysis must broadly account for all of the seller’s communications about the token sale, not just formal materials such as the white paper and terms of sale.

Moreover, state law may play a role in the level of risk for any given token sale under U.S. securities laws. Every state maintains its own securities laws, known as “Blue Sky Laws,” which aim to protect investors from fraud. Although the SEC garners most of the attention when it comes to securities regulations as applied to token sales in the United States, the state of Texas reminded the industry that token sale operators should also mind state Blue Sky Laws. The Texas Securities Commissioner issued an emergency cease and desist order on January 4, 2018 requiring BitConnect to stop offering any securities for sale in Texas until BitConnect either registers with the Texas Securities Commissioner or receives an exemption under the Texas Securities Act.\textsuperscript{100} The Texas Securities Commissioner determined that BitConnect should have registered in Texas before making sales to Texas residents and that BitConnect failed to disclose material information to the investors it solicited in Texas.\textsuperscript{101} The action against BitConnect reminds those operating a token sale in the United States that state regulators have both similar concerns and similar enforcement tools as their federal counterparts.

On the other hand, tokens that do not constitute investment contracts under U.S. securities law may constitute commodities, which fall under the jurisdiction of the Commodity Futures Trading Commission (“CFTC”). The Commodity Exchange Act (“CEA”)\textsuperscript{102} gives the CFTC jurisdiction over certain kinds of transactions involving commodities, generally those involving commodities derivatives, future delivery, or financing, leverage, or margin. As a point of reference, the CFTC has stated that a virtual currency is a commodity for purposes of the CEA.\textsuperscript{103} The question of whether the CFTC would assert jurisdiction over smart contract-based tokens thus turns on whether (i) the CFTC would construe a particular token as either a virtual currency or other commodity under its purview, and/or (ii) whether transactions involving such tokens fit into any of the types of transactions over which the CFTC has jurisdiction. On December 15, 2017, the CFTC issued a proposed interpretation of the term “actual delivery” as used in the provision of the CEA that grants the CFTC explicit authority to oversee the marketplace for “retail commodity transactions.”\textsuperscript{104} Commentators believe that it is not merely a coincidence that the proposed interpretation was issued just days after trading in bitcoin futures contracts began.\textsuperscript{105} Rather, the two are connected by the regulatory principle underlying the CFTC’s oversight of retail commodity transactions: “such arrangements are speculative in nature and have indica of futures contracts by virtue of the use of leverage, margining or financing.”\textsuperscript{106} Thus, “[m]argin, leveraged or financed transactions involving virtual currency entered into by retail investors are regulated by the CFTC as ‘retail commodity transactions.’ When a centralized virtual currency exchange or trading platform (‘Platform’) offers margin trading, or facilitates margin, leveraged or financed virtual currency transactions on behalf of its retail investors, the Platform is subjected to CFTC oversight unless there is ‘actual delivery’ of the purchased virtual currency within 28 days of the transaction.”\textsuperscript{107}

\textsuperscript{98}Id. 5-8.
\textsuperscript{99}Id. at 8 (citing Forman, 421 U.S. at 849; SEC v. C.M. Joiner Leasing Corp., 320 U.S. 344, 352-53 (1943) (indicating the “test . . . is what character the instrument is given in commerce by the terms of the offer, the plan of distribution, and the economic inducements held out to the prospect!”)).
\textsuperscript{101} Id. at 5-8.
\textsuperscript{102} 7 U.S.C. § 1 et seq.
\textsuperscript{105} Id.
\textsuperscript{106} Id.
To determine whether virtual currency is actually delivered within 28 days, the CFTC intends to take a “functional approach.” By taking a functional approach, the CFTC means that actual delivery in the context of virtual currency will be met by the following requirements: 1. there be a record on the relevant public distributed ledger network or blockchain of the transfer of the entire quantity of the virtual currency to the purchaser’s blockchain wallet; 2. the purchaser be able to freely use the virtual currency (both within and away from any particular Platform); 3. neither the counterparty seller nor the Platform retains any interest in or control over the transferred virtual currency; and 4. the counterparty seller has transferred title to the purchaser, which may be reflected by linking the purchaser with proof of ownership of the wallet into which the virtual currency is transferred. This interpretation of the term “actual delivery” is merely a proposed interpretation, and the public has 90 days from the date the proposal is published in the Federal Register to comment.

This proposed interpretation is not the only way the CFTC is demonstrating active policing of the virtual currency market. On January 19, 2018, the CFTC filed two civil enforcement actions—one in Colorado and one in New York—both alleging deceptive and fraudulent conduct on the part of purported virtual currency-related business operators. Then, on January 24, 2018, the CFTC announced an enforcement action against two individuals and My Big Coin Pay, Inc., alleging commodity fraud and misappropriation in connection with selling a fake virtual currency. The two individuals and My Big Coin Pay, Inc. allegedly misappropriated over $6 million from consumers by accepting the funds without actually providing a service or product to the consumers in return, and then siphoned the funds off for personal use. These enforcement actions came in quick succession and were made public right around the same time that CFTC Enforcement Director James McDonald and SEC Enforcement Co-Directors Stephanie Avakian and Steven Peikin made a joint statement emphasizing that “[w]hen market participants engage in fraud under the guise of offering digital instruments—whether characterized as virtual currencies, coins, tokens, or the like—the SEC and the CFTC will look beyond form, examine the substance of the activity and prosecute violations of the federal securities and commodities laws.” The SEC and CFTC also issued a joint op-ed around the same time that emphasized their mutual intent to more strictly monitor token sales and enforce against unregistered sales of tokens deemed to be securities, in addition to fraudulent and other criminal activities. Then, in early February 2018, the Chairman of the SEC and the Chairman of the CFTC both testified at a hearing of the United States Senate Committee on Banking, Housing and Urban Affairs entitled “Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission.” The testimony evidenced continued collaboration between the two agencies and a commitment to the enforcement of existing laws in the token sale space. Regulatory activity by both the SEC and the CFTC therefore remains an issue to watch carefully, and by no means does it exhaust the regulatory quagmire potentially applicable to token sales.

For example, in other scenarios, where a smart contract or token serves as a digital representation of ownership of goods, the token may simply represent an electronic “document of title” as described in Article 7 of the Uniform Commercial Code. Other legal constructions that may be appropriate for DLT tokens include that of a system license or a franchise law framework.
Furthermore, those offering either a protocol token or a utility token as part of their product and service model should carefully consider the potential application of money transmission laws. Although the securities and commodities issues receive much of the current public attention, the issuance of protocol tokens, whether consumable or not, may trigger regulation as a money transmitter or prepaid access provider under relevant federal and state laws. In March 2013, the U.S. Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”) issued its seminal guidance on the application of the Bank Secrecy Act (“BSA”) and its implementing regulations to virtual currencies (the “Virtual Currency Guidance”). The Virtual Currency Guidance outlines the applicability of the BSA regulations relating to anti-money laundering (“AML”) requirements to decentralized virtual currencies, “and concludes that administrators and exchangers of such currencies are subject to the AML requirements to the extent that they transmit decentralized virtual currency or legal tender from one user to another, or from one location to another.” As explained in the [Virtual Currency] Guidance, a person is an exchanger and a money transmitter if the person accepts convertible virtual currency from one person and transmits it to another person (or location) as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency. FinCEN takes the position that even if the transmission of value is between two different accounts (or wallets) of the same person, the BSA AML regulations apply. Thus, a token sale may trigger regulation under the BSA as a money transmission. Some states take a similar position. In the context of a token sale, the token seller typically accepts convertible virtual currency from one person and transmits a token back to that person. The extent to which this exchange triggers money transmission regulation in any given token sale may rest on the technical details of the token sale, such as how an ERC20 contract used for Ethereum-based tokens is constructed. In general, the more control the token seller has over the smart contract, the greater the risk. As a result, those conducting token sales should carefully consider their legal obligations under both state and federal money transmission laws, in addition to the securities and commodities law considerations discussed above. In particular, with respect to state law, industry participants should remain vigilant for changes to the state money transmitter laws that may impact their operations. Some of these changes may involve increased uniformity of state laws. For example, the Uniform Law Commission approved and recommended the enactment of the Uniform Regulation of Virtual-Currency Business Act (“URVCBA”) in July 2017, and two states—Hawaii and Nebraska—introduced the URVCBA for consideration by their legislatures in the first months of 2018.

In addition, depending on the nature and legal characterization of a token based on smart contract functionality, sales of tokens present novel tax questions—which as part of a crowd sale or fundraising effort or as an independent transaction. These tax issues include questions such as how to characterize the digital asset for taxation purposes, how to assign a value or cost basis to token sales when only digital assets (i.e., no fiat currencies) are exchanged (particularly in the context of a crowd sale), and how to assign a jurisdiction to the issuance or exchange for taxation purposes. Answers to these tax questions may, in turn, influence the jurisdiction in which development teams who are building smart contract platforms and applications may choose to incorporate.

Finally, all U.S. citizens and legal permanent residents (i.e., green card holders) anywhere in the world, all companies organized in the United States, all foreign branches of U.S. companies, and any person or entity located in the United States (“Covered Persons”) involved in a token sale with worldwide scope must remember that they are subject to the regulations enforced by the Office of Foreign Assets Control (“OFAC Regulations”) governing U.S. sanctions. Covered Persons may not be involved in, or in any way facilitate, a transaction that violates OFAC Regulations and U.S. sanctions. Although the specific OFAC Regulations vary by sanctions program, in general, they prohibit Covered Persons from brokering, financing, guaranteeing, approving, or selling anything to persons residing in sanctioned jurisdictions or that are identified on the Specially Designated Person’s List.

125 FinCEN, Virtual Currency Guidance, supra note 122.
128 Id.
SMART CONTRACTS IN CAPITAL MARKETS

How Are Smart Contracts Used in Capital Markets?

The potential uses of smart contract applications in capital markets include tokenized securities, syndicated loans, cash equities, collateral tracing, and leveraged loan trading. With regard to cash equities specifically, a recent Goldman Sachs report details the potential for smart contracts to “drive greater efficiencies in the US cash equities market, primarily through streamlining the post-trade settlement and clearing processes.”129 Goldman Sachs envisions smart contracts will be used to “eliminate[d] duplicative confirmation/affirmation steps, shrink[ing] trading risk, which in turn should lower the industry’s cost and capital needs."130 In total, Goldman Sachs estimates that the use of smart contracts in these ways could result in approximately $2 billion in cost savings in the United States alone, with approximately $6 billion in cost savings globally.131 Market participants are already exploring these applications. In particular, “issuers have contemplated the issuance of securities represented digitally rather than by a share certificate.”132 Additionally, the “DTC and its parent, Depository Trust & Clearing Corporation (DTCC), have committed to achieve blockchain-based enhancements to their processes.”133

Some actors are pursuing the issuance of tokenized securities in order to leverage the token sale trend to sell what is explicitly recognized as a security by everyone involved. For example, the venture capital firm Blockchain Capital sought to conduct its own, regulatory-compliant sale of tokenized securities. The venture capital firm released the offering memorandum for a $10 million fundraise through a month-long sale of tokenized securities in early April 2017;134 the tokenized security sale began April 10, 2017,135 with token issuance to occur on May 10, 2017, and the firm raised its $10 million in just six hours. The sale was conducted by an entity incorporated in Singapore, where the Monetary Authority of Singapore’s 2014 guidance on token sales helped provide regulatory clarity.136 Blockchain Capital availed itself of the registration exemptions afforded by the SEC under Regulations S and D to allow the sale to raise money from international investors and U.S. accredited investors.137

The idea of issuing securities represented digitally rather than by a share certificate made significant advancements in 2017. After the entry of a class settlement in the Delaware Court of Chancery shareholder action In re Dole Food Co.,138 the court, class action attorneys and the Depository Trust Company (“DTC”) were unable to determine which individuals were the current owners of the class shares.139 “In re Dole Food Co.’s main culprits for the discrepancy were delays in registering trades and short-selling.”140 In a footnote, In re Dole Food Co.’s presiding judge commented that blockchain technology could be put to use in alleviating these problems.141 In response, after significant study and consideration, the Delaware legislature recently amended the Delaware General Corporate Law to recognize tokenized securities issued by companies incorporated in Delaware.142 The DLT-related changes include amendments to Sections 151(f), 202(a), 219(a), 219(c), 224, 232(c) and 364 of the Delaware General Corporate Law. “Amendments to Sections 219, 224 and 232 and related provisions are intended to provide specific statutory authority for Delaware corporations to use [DLT] for the creation and maintenance of corporate records, including a corporation’s stock ledger.”143 Other amendments specify the requirements for a stock
ledger, which are intended to ensure that only DLT protocols that possess certain characteristics will suffice for use in issuing corporate shares.144

**Legal Aspects of Using Smart Contracts in Capital Markets**

Although the changes to the Delaware General Corporate Law represent a significant advance in the ability of companies to consider issuing shares through DLT, challenges remain. First, the amendments "only facilitate issuance of new shares registered on a distributed ledger. For existing shares, transition to distributed ledger would be more complicated, since only uncertificated shares would qualify."145 Further, since the state corporate statute only affects transfers of record, trading shares on secondary markets seem to be unaffected by the changes to the Delaware law.146 It is unclear how and whether secondary markets will be open to Delaware companies that elect to issue shares through DLT. In particular, “none of the existing Stock Exchanges are currently set up to trade digital securities.”147 One alternative can be found in Overstock’s Alternative Trading System ("ATS") that is designed to trade digital securities, which was created as an SEC-regulated broker-dealer trading system.148 Others could use that ATS or create similar ATS vehicles if a demand emerged.149 In other words, although obstacles remain, the amendments to the Delaware General Corporate Law appear to create a viable pathway from a legal perspective. As a result, the effective adoption of digital shares under the Delaware amendments “will depend on the perceived value of this new paradigm compared to the challenges it poses.”150

**SMART CONTRACTS FOR SUPPLY CHAIN MANAGEMENT**

**Why Are Smart Contracts of Interest for Supply Chain Management?**

The “supply chain” refers to “all the links involved in creating and distributing goods, from raw materials to the finished product that goes into the possession of the consumer.”151 When the idea of the supply chain originally emerged, it “was a revolutionary idea that would improve visibility and control on goods and products as they moved from point A to point B.”152 Today’s economy involves a new type of supply chain—one that is more fragmented, more complicated, and more geographically diffuse.153 “In effect, the supply chain is now an opaque and faulty process that is extremely hard to manage.”154 As a result, neither intermediate buyers nor the ultimate consumers are able to reliably confirm the value of the goods and services they purchase.155 Further, attempts to enforce laws relating to counterfeit goods, forced labor, poor working conditions, or connections to criminal activities are stymied due to the global reach and massive scale of most supply chains.156 In other words, a new technology is needed to help control the effects of the technology at work in today’s global supply chains. Many believe DLT can be that technology.157

---

144 Id.
146 Id.
147 Ness & Bystrowicz-Liendo, supra note 143.
148 Id.
149 Id.
150 Id.
According to IBM, “[o]ptimizing a supply chain on the blockchain makes new things possible, such as the real-time synchronization of decisions with supply chain partners.” By doing so, companies may be able to significantly mitigate many routine difficulties in supply chain management. Specifically, a bitcoin or other decentralized virtual currency would serve as a unit of inventory, and a wallet would serve as an inventory-keeping location, such as a store, distribution center, or truck trailer. Under such an arrangement, the blockchain “could be used to record the balances and transfers of inventory across a distributed supply chain network.” DLT could also be used to help asset owners trace the quantity and transfer of assets as they move between elements in the supply chain. In supply chains where provenance is important, DLT could also be used to prove the source of materials, prevent fraud and enhance capacity for accurate freight audits.

In one implementation of this idea, a service “enables every physical product to fraud with a digital ‘passport’ that proves authenticity (Is this product what it claims to be?) and origin (Where does this product come from?), creating an auditable record of the journey behind all physical products.” The service “details four key properties concerning all materials and consumables it covers: the nature (what it is), the quality (how it is), the quantity (how much of it there is), and the ownership (whose it is at any moment). Key attributes may be read and linked from pre-existing datasets such as barcodes, or newly ascribed along the way.” The idea is that this system allows for an unprecedented breakthrough in supply chain management—the unbroken chain of custody from the raw materials to the end sale.

In a concrete example, IBM announced a program in 2017 in which, in partnership with Walmart, Nestlé, Dole, Tyson Foods, and Kroger (among others), it is building a platform “to use blockchain technology to track food throughout the complex global supply chain.” The goals of such programs include reduction or elimination of fraud and errors, improved inventory management, reduced courier costs, reduced delays from paperwork, faster identification of issues, and enhanced consumer and partner trust. Ultimately, the IBM program, like the other programs discussed above, seeks to use blockchain to “digitally trace and authenticate . . . products from an ecosystem of suppliers to store shelves and ultimately to consumers.”

Legal Aspects of Using Smart Contracts in Supply Chain Management

The Dodd-Frank Wall Street Reform and Consumer Protection Act imposes supply chain responsibility obligations on all publicly held companies. Additionally, the California Transparency in Supply Chains Act imposes obligations on entities that “do business” in California and have annual sales of $100 million or more. Furthermore, companies importing or exporting products across borders must deal with shipping regulations, embargo laws and regulations, export sanctions, anti-corruption and foreign corrupt practices laws, anti-money laundering requirements, anti-boycott laws and regulations, and trade remedy laws and regulations. Additional compliance concerns are raised by the Foreign Corrupt Practices Act, the U.K. Bribery Act, the U.S. Federal Acquisition Regulations on Trafficking in Persons in Federal Contracts, the U.K. Modern Slavery Act of 2015, the European Union’s Directive on Transparency and its amendments, and the proposed U.S. Business Transparency on Trafficking and Slavery Act, among other laws. A business that is developing and providing DLT-based supply chain management software would be well served by staying informed of the legal context in which its supply chain clients must operate to ensure that the software it provides sufficiently enables such clients to comply with the relevant regulatory obligations.

---

262 Id. at Blockchain and Food Traceability Infographic.
263 Id. for other services in the supply chain space, see Blockverify (http://www.blockverify.io/), which is providing a way to verify the authenticity of medicine; Everledger (https://www.everledger.io/), which is trying to bring transparency to the diamond supply chain; and Kouvola Innovation (https://www.koinno.ifi/), which seeks to provide a smart tendering solution for the supply chain.
266 See IBM Blockchain, supra note 167.
267 Id. at Blockchain and Food Traceability Infographic.
Reports of governments investigating the use of recordkeeping systems deployed on the blockchain abound; such governments include the United Kingdom, Estonia, Dubai, the U.S. federal government, and various state governments in the United States (e.g., Vermont, Delaware, and Illinois). Some government interest can be attributed to a belief in DLT’s capacity “to vastly reduce the cost and complexity of getting things done.” Generally speaking, government leaders expect that a DLT-based system “will be faster and cheaper than the existing process since it automates a number of processes.” Others feel that in addition to enhancing the transparency, security, and efficiency of existing government services, DLT-based government records may create opportunities to offer additional government services not previously possible. Possibilities for revamping the U.S. personal property filing system used to record secured transactions conducted under Article 9 of the Uniform Commercial Code (“UCC”) and for making Bank Secrecy Act compliance less burdensome have also been suggested. In fact, the European Union is presently exploring DLT’s potential to lessen compliance burdens in the financial services industry.

Delaware again offers a prime example of a state government moving toward smart governance through DLT. In addition to the changes made to its corporate law, Delaware, through its Blockchain Initiative, piloted a program to store the Delaware public archives on a DLT recordkeeping system. Delaware then used that system as the basis for building a DLT-based filing system for the receipt and management of UCC-1 forms. Lenders with security interests in the property of a debtor file UCC-1 forms under UCC Article 9 to establish priority in repayment and to announce to any other interested parties the existence of the loan and their interest in the collateral. The existing UCC-1 filing system is beset by a number of inefficiencies that make it cumbersome and expensive to use effectively. A DLT-based UCC-1 filing system offers hope for reducing those inefficiencies, lowering costs, and improving access to information, thereby reducing related litigation.

In another very concrete example, the State of Illinois’ Department of Innovation and Technology put out a request for information that designated four specific areas of interest: (1) identity, attestation, and ownership registries; (2) compliance and reporting ledgers; (3) benefit and entitlement ledgers; and (4) new products and other areas of interest. With regard to the first area of interest, Illinois is investigating how it could use DLT “to consolidate disparate data that currently exists across multiple agencies and layers of government into a single self-sovereign network centered around the citizen,” and whether “a persistent, secure identity layer [could] allow Illinois to more efficiently deliver private, secure, reliable, and integrated services.”

---

219 Reyes, supra note 3.
220 DIEDRICH, supra note 16.
222 Id. For further analysis of the Delaware Blockchain Initiative and other similar government endeavors, see Carla L. Reyes, Blockchain-Based Agencies, 42 ADMIN & REGULATORY L. NEWS 9 (Summer 2017).
224 Id. at 402-03 (citing LoPucki et al., supra note 187, at 281-92, 294-95).
225 Id. at 408; Tinianow & Long, supra note 185.
226 Holloway, supra note 178, at 5-6.
227 Id. at 5.
With regard to compliance and reporting, Illinois queries whether DLT can “enable businesses and individuals either required to report information or voluntarily providing information, a more trusted, transparent yet anonymous way of doing so,” and whether “these reporting ledgers [could] help limit reporting to one trusted, verifiable source provided by the entity involved.”

In the realm of benefits and entitlements, Illinois hopes to leverage DLT to reduce fraud and allow more efficient distribution while also increasing transparency. Finally, the State of Illinois also indicated a broader interest in learning about (a) other DLT-as-a-service products, including escrow, digital notaries, public records management, and digital identities; (b) possibilities for a public permissioned blockchain with network nodes and participants authenticated by the state government; and (c) using DLT to secure IoT infrastructure from cybersecurity threats.

The most expansive plans to use DLT and smart contracts to enable smart government and smart cities belong to the Dubai government. Dubai’s stated goal is to be the first government in the world to execute all applicable transactions on DLT-based systems by 2020. Achieving this goal would make Dubai the first government to pioneer DLT on a citywide scale. To that end, Dubai launched a program of flying startup companies from around the world to pilot blockchain use cases for its government. In a coordinated government agency effort, Dubai hopes to enable DLT-based systems for energy and water, transport and logistics, economic development, tourism, safety and justice, municipality and land, health, social services, and smart districts. Ultimately, Dubai envisions its DLT-based government smart record and smart city program as the path to achieving key policy objectives, including creating a lean, connected government, enabling a globally competitive economy, supporting a high quality of life, enhancing financial and economic efficiency, and improving resource and infrastructure efficiency. Key components of this plan involve using smart contracts in several of the other ways discussed in this white paper: to protect identity, to trace property ownership, to improve supply chain management, and to disrupt capital markets.

Since its launch of this effort in October 2016, Dubai has established the Smart Dubai Office Blockchain Challenge in partnership with global accelerator 1176, launched its own Smart Dubai Office Accelerator at the Dubai Future Accelerators, and announced initial contract awards for IBM and Consensys. In March 2017, Dubai officially kicked off “Smart Dubai”—a citywide effort to implement blockchain. In the months that followed, Smart Dubai held multi-stakeholder workshops to create a work plan for the services best suited to reform by DLT. Smart Dubai hopes to roll out initial pilot systems this year, and to build a “Blockchain as a Service” platform for various Dubai governmental entities to use in building their own pilot projects. In one example of such efforts, in October 2017, Dubai announced plans to launch “emCash,” a digital currency rooted in DLT. Built by Emcredit, a subsidiary of Dubai Economy (an arm of the Dubai government), and Object Tech Grp. (a UK-based startup), emCash will be redeemable for services offered by both government and private sector providers. Essentially, emCash can be seen “as a local currency with a fixed price backed by the government and accepted by all merchants in the city built on a blockchain.” By all accounts, Dubai’s plans for smart government recordkeeping and a smart city are moving forward according to schedule.

The extent to which any government incorporates smart contracting features into the DLT-based smart records application it chooses to adopt depends entirely on the government, its goals, and the particular needs of the application. At one end, a smart records program might focus entirely on the time-stamping and immutability functionality of DLT protocols; such programs might be considered a highly efficient notary and recordkeeping service with extreme transparency. At the other extreme, “an enterprising locality could offer a blockchain-based municipal bond that automatically accrues and pays interest to its holder on a pre-determined schedule.”
Legal Aspects of Using Smart Contracts for Smart Records and Smart Cities

Using smart contracts and DLT protocols in the context of government recordkeeping may raise important questions of administrative law.205 Given the inherent difficulties of correctly programming smart contracts applications, “[w]hat remedies will belong to the governed when the computer code makes an unexpected or undesirable decision, or both? Who will be at fault if the code executes prematurely because it misread the circumstances?”206 Although the administrative law burdens will fall to the state agencies embarking on a smart records project, those developing DLT-based programs that incorporate smart contract features for government use must carefully negotiate their contracts with the hiring agency and pay particular attention to questions of liability for product malfunction and unexpected consequences. Furthermore, the more complicated the software programming required, the more likely the philosophies (and, at times, biases) of the software developer are to infuse the code. “[E]xtensive research evidences the extent to which developers frequently write implicit biases into the code and algorithms they create.”207 As a result, those businesses offering software-as-a-service solutions to governments seeking to implement a smart records regime must remain vigilant and cognizant of laws relating to anti-discriminatory practices conducted by the government.

SMART CONTRACTS FOR REAL ESTATE REGISTRIES

Why Are DLT-Based Real Estate Registries Needed?

Around the world, governments manage real property ownership rights through public land registries. Such registries, effectively operated as a centralized ledger, suffer from significant flaws, even in industrial countries, where a complicated system of real estate law has developed.

In many developing countries, land registry systems remain inefficient, inaccurate, and bloated with inequities and corruption, and in some cases, they do not functionally exist at all. In his groundbreaking book The Mystery of Capital, economist Hernando de Soto argued “that the major stumbling block that keeps the rest of the world from benefiting from capitalism is its inability to produce capital.”208 De Soto posited that although the world’s poor “already possess the assets they need to make a success of capitalism . . . they hold these resources in defective forms,” such as real property without proper title.209 The idea is that because the assets are not held by title, they “cannot readily be turned into capital, cannot be traded outside of narrow local circles where people know and trust each other, cannot be used as collateral for a loan, and cannot be used as a share against investment.”210 Without proper title, an enabling mechanism for leveraging assets, the assets held by the poor members of developing nations are “dead capital,”211 useless for wealth generation and a stumbling block to economic development. Many believe that DLT offers an alternative method for registering and tracing real estate ownership interests more accurately and efficiently. Another claim is that blockchain-based land registries offer the opportunity to democratize real estate ownership interests by putting control over the record into the hands of the owners and thereby limiting the effect of corruption and politics that otherwise jeopardize land registries in many developing countries.212

---

205 Reyes, supra note 3, at 423.
206 Id. at 425.
207 Id. at 426 (citing FRANK PASQUALE, THE BLACK BOX SOCIETY 110-13 (2015)).
209 Id. at 5-6.
210 Id. at 6.
211 Id.
212 Id. at 11, 16 (“The institutions that give life to capital—that allow one to secure the interests of third parties with work and assets—do not exist here.”). Earlier in his career, De Soto explained the idea in terms of his native Peru as follows: “So far, we have seen that Peruvians are forced to assume excessively high costs in order to operate legally or, if they are unable to do so, that they have been left out of the system. This means that they cannot take advantage of the country’s good laws, namely the facilitating instruments provided by the law to make economic and social activities more efficient: property rights, contracts, and extracontractual law.” HERNANDO DE SOTO, THE OTHER PATH: THE INVISIBLE REVOLUTION IN THE THIRD WORLD 177 (June Abbott trans., 1990).
Where Are DLT-Based Land Registries Being Developed?

Examples of blockchain-based land registry proposals abound. The Economist reported that Factom partnered with the government of Honduras in 2015 to build a more effective land registry there, where “land registries are badly kept, mismanaged and/or corrupt,” as they are “across much of the world.”213 The Republic of Georgia engaged the Bitfury Group “to advance transparency by developing a system for registering land titles using the Blockchain for the National Agency of Public Registry.”214 The chairman of Georgia’s National Agency of Public Registry reportedly described Georgia’s interest in building a blockchain-based land registry as follows:

> By building a Blockchain-based property registry and taking full advantage of the security provided by the Blockchain technology, the Republic of Georgia can show the world that we are a modern, transparent and corruption-free country that can lead the world in changing the way land titling is done and pave the way to additional prosperity for all.215

Greece has also expressed interest in developing a blockchain-based land registry; in Greece “only 7% of the territory is adequately mapped.”216 The Swedish National Land Survey unveiled its own plans to partner with ChromaWay to test a system for registering and recording land titles in an effort to digitize its real estate process.217 In West Africa, Bitland Global (“Bitland”) is developing a land registry system designed to “provide immutable records of ownership to those who normally would have difficulty” obtaining such records.218 Located in Kumasi, Ghana, Bitland is a nonprofit organization “working to keep the land registration process accessible, transparent, and free from government corruption” by updating “paper data storage houses into digital format,” consolidating “new land registry requests against the old registries,” and integrating systems that local communities have developed for keeping track of titles.219 And lest the United States feel left out of the movement, The Office of the Cook County Recorder of Deeds in Cook County, Illinois participated in a pilot program during the last several months of 2016 through May 2017.220 Although the Cook County Recorder of Deeds ultimately determined that a DLT-based land registry and mortgage recording system could provide certain efficiencies and decrease the potential for fraudulent transfers, the resource-intensive nature of a DLT-based system and the reality of local politics led the office to conclude that it should not further pursue a DLT-based system until around 2020.221

These DLT-based land registries rely upon the smart contract capabilities of DLT protocols. The general idea is that DLT-based land registries can leverage the capacity of smart contracts to record state changes in real estate ownership and then immutably record those changes on the chosen DLT protocol. Some of the land registry projects under development rely on public DLT protocols, while others are designed for private DLT protocols, and still others, like that of ChromaWay, are protocol and consensus-neutral such that they can be deployed on any underlying DLT protocol. By recording the changes in land ownership on a DLT protocol, these land registry projects also offer an accountability mechanism—namely, “every user of [the] service can reliably verify that the service operates in the intended way (e.g., information provided by the service agrees with the information it provided to other users).”222 Although the possibility of an immutable audit trail offers an attractive reason for moving land registries to DLT, DLT does not automatically solve the problem of ensuring that the data originally entered into the ledger is accurate and reliable—it merely ensures that once the data is entered, state changes to that data can be traced going forward.223

---

216 Blockchains, supra note 215.
221 Id. at 3-4.
Legal Aspects of DLT-Based Land Registries

The most critical and obvious legal aspect of DLT-based land registries centers on the fact that most public land registries are controlled by government actors. Thus, to be legally effective, land registry processes must be developed in connection with or on behalf of the relevant government actor. Alternatively, the company might develop a platform and allow governments to adopt it as they please. Regardless of how the DLT-based land registry is adopted by the appropriate government actor, both the government and the application developer should remain cognizant of the implications that doing so will have for real estate law more broadly. Developers should be prepared to explain to their government clients how the DLT-based system interacts with, and in some respects, might replace, the existing real estate laws. Further, where the DLT-based land registry is offered on a software-as-a-service (“SaaS”) basis, the company should consider traditional legal issues applicable in the SaaS context, including licensing, software code escrow, privacy and security, redundancy systems, and system-level agreements, among others. A detailed description of the issues involved in each of these areas is beyond the scope of this white paper; however, companies offering DLT-applications in this area would be well served by consulting experienced technology transactions counsel before launch.

SMART CONTRACTS FOR ENABLING SELF-SOVEREIGN IDENTITY

How Can Smart Contracts Enable Self-Sovereign Identity?

Many observers think that DLT offers an opportunity to create and validate digital identities that could replace current physical forms of identification such as a passport or driver's license. In the digital economy, a person's identity is often fragmented across government agencies, service providers, and business entities. Often people jeopardize the security of their own identities by using the same user name and password across platforms for ease of memory. Furthermore, the person does not retain full control of all of the pieces of their own digital identity. Instead, the person gives up control of certain identity data to the service provider, ultimately meaning that the service provider can revoke the person's access to such data. Such revocation could, in turn, impact access to other services that is predicated upon the digital identity that has been revoked.

For example, major social networks allow a person to build a trusted digital identity by allowing that person to use his or her login credentials for their services as a proxy to log in to other services. But if a major social media platform deactivates a person's account, that person loses the identity he or she created on that social media platform, which could put at risk the trusted nature of his or her online identity with a host of other providers.

In this context, an ideal form of digital identity has been described as a self-sovereign identity. A self-sovereign identity would offer a person control over his or her identity (including who has access to what aspects of his or her identity), would be protected from unauthorized use or disclosure, and would be portable—namely, capable of use by the person to identify himself or herself without seeking permission from or being tied to a service provider, and capable of being transferred freely without being at risk of loss. Holistically, a self-sovereign identity can be thought of as a repository of identity data about a person where data that supports proof of that person’s unique identity can be added by the identity owner or by others at the identity owner’s request.

DLT is thought to enable self-sovereign identity in ways that were previously not feasible. DLT allows the creation of a digital fingerprint by linking “attributes” to a self-sovereign identity. “Attributes” (which are also sometimes called “claims”) are descriptors of a person, such as the person’s name or birthdate. DLT also allows other entities to verify a person’s attributes (also sometimes referred to as an “attestation”), which, in turn, allows that person to use the verified attribute in other circumstances.

---

224 For a more thorough review of how a government might, in line with administrative law constraints, adopt a DLT-based application that takes a traditional government process and moves it to a DLT-based process, see Reyes, supra note 3.
225 For an in-depth consideration of how to undertake such considerations, see id.
228 Tobin & Reed, supra note 228, at 9.
For example, if a person’s name and social security number are attested to by a bank, then a subsequent bank can rely on that attestation without having to independently conduct the same verification. The DLT protocol provides a security level for self-sovereign identity. DLT protocols make it exceedingly difficult for a single entity to make changes to recorded transactions without the nodes on the network becoming aware of the change and rejecting it. Perhaps recognizing the potential benefits of using a DLT-based system to provide digital identity service, the United Nations High Commissioner for Refugees (“UNHCR”) teamed up with Accenture and Microsoft, as part of ID2020, to create a digital ID network powered by DLT. The system “connects existing public and commercial records so people can access their personal details from any location.”

Legal Aspects of Using Smart Contracts for Self-Sovereign Identity

Using a system of self-sovereign identity built on DLT protocols will allow individuals to benefit from the security and privacy built into DLT’s cryptographic nature, and it may also limit a business’s risk of liability for data breach or mishandling of personal data by enabling it to rely solely on attestations that have been signed to the ledger, and not collect any data itself. However, certain data privacy laws may be incompatible with the immutable nature of the digital identities anchored in a DLT protocol. For example, European citizens have a “right to be forgotten,” and the U.S. Fair Credit Reporting Act, the Gramm-Leach Bliley Act, and the SEC’s Regulation S-P mandate that personal financial data be easily redacted. Further, to the extent that any self-sovereign identity solution links biometric data to the system, there are a number of privacy laws in the United States that either specifically govern biometric data or are broad privacy laws under which biometric data may fall. Generally speaking, such laws regulate third parties’ use and collection of biometric data. Some states even regulate how digital accounts are handled after the owner dies, and others are actively attempting to pass such legislation. Such laws raise the question of how to treat a self-sovereign identity repository or account after the person to whom the identity belongs is deceased.

Moreover, there is some concern that, depending upon the design of the DLT-based digital identity system, a more centralized identity repository may emerge, rather than the intended self-sovereign identity paradigm. In particular, Brandie Nonnecke, of the Center for Information Technology Research in the Interest of Society, argues that as biometric data is tokenized, a token service provider could amass a significant amount of biometric data that may pose a greater cybersecurity risk than intended. In the UNHCR digital identity program, for example, the UNHCR and Accenture built a Biometric Identity Management System (“BIMS”) to enable relief agencies to more easily share information. Even though the BIMS is a DLT-based system, “as biometric and personal data are collected by UNHCR and shared with third parties, there’s the possibility that this data could be transferred to privately controlled databases, raising the risk of data being compromised or stolen.” The risk of liability from such data centralization and related potential data breaches must be considered before moving forward with an identity product launch.

Further, to the extent that financial institutions rely on attestations or other elements of a self-sovereign identity to meet compliance obligations under the anti-money laundering provisions of the Bank Secrecy Act, what happens if the self-sovereign identity service provider makes an error or the code suffers from a flaw that compromises the integrity of the attestations? In light of the complexity of coding smart contracts to accurately execute according to the designers’ intended purpose, complex issues of fault, liability, and remedies may arise. Any company beginning the planning phase of a product launch in this area would do well to carefully consider each of these issues throughout the product life cycle.

---

233 For a discussion of how privacy interests are traditionally terminated at death and an exploration of how they should be revived and reshaped in a digital future, see Natalie M. Banta, Death and Privacy in the Digital Age, 94 N.C. L. REV. 927 (2016).
236 Nonnecke, supra note 236.
IV. AN INITIAL RISK MITIGATION CHECKLIST FOR BUSINESSES DEVELOPING SMART CONTRACTS APPLICATIONS

Although smart contract-based applications vary greatly, sufficient common elements exist to enable the companies developing them to be proactive in reducing their risk of liability exposure. We offer a preliminary, non-exhaustive checklist of such issues here, and we recommend that companies in this area reach out to experienced legal counsel at each stage of application development: when contracting with customers, when building and testing the application, and before moving the application to public deployment.

Practical issues to consider with legal counsel when developing smart contracts applications include, but are not limited to:

- What is the legal context in which the smart contract application will operate?
- Will the smart contract replace any function previously performed by government actors? If so, what features of the law need to be replicated in the application to protect the validity of the transaction, and how should the user (a state actor) expect the law to change in response to use of the smart contract application?
- What laws otherwise apply to the transactions taking place within the application? Does the application allow parties to comply with their obligations under those laws?
- What hazards are posed by use of the smart contract application alone (e.g., can you be held liable for a (i) a loss of data; (ii) business interruption; (iii) privacy breach; and/or (iv) a failure to perform)?
- What hazards are posed by using the smart contract application with other software (e.g., can a party be held liable for a flaw in the software that causes the smart contract to fail)?
- Are there hazards that should be designed or guarded against?
- Do you owe any duties to any other parties involved in the smart contract application?
- If you have a duty to warn, what warnings or instructions are necessary and/or advisable?
- How should a warning be communicated in order to limit liability exposure if the application malfunctions?
- Do you have a protocol or system of monitoring in place to assist your software developers in guarding against coding implicit biases into the smart contract application?
- Do you have an incident response plan to control and mitigate any failure in the application or breach?
- Do you have a protocol in place to capture the data that you will need to quantify any loss or liability?
- What contractual provisions do you need to limit liability and maximize the availability of indemnification?
- Have you considered and properly contracted around issues unique in the software-as-a-service context?
- Have you considered and properly contracted for software code audit services?
- What privacy and security law considerations do you need to bake into the smart contract application?
- Have you considered what insurance you need to protect your business from loss and liability exposure associated with smart contract applications, and whether your application would benefit from specially crafted (or “manuscripted”) coverage (e.g., errors and omissions insurance) that is tailored to your business model?

V. CONCLUSION

In sum, smart contracts will continue to evolve as a technology, and the legal issues surrounding the technology will likewise continue to evolve and involve novel questions beyond simply contract law. We predict that smart contracts will continue to disrupt, from both a technological and legal perspective, digital asset sales, venture capital and capital markets, supply chain management, government and smart cities, real estate registries, and self-sovereign identity, as well as other use cases not yet imagined. Although legal risk remains inherent in any technology platform, we conclude that companies who engage in careful planning can and will effectively mitigate these legal risks while offering products and services that utilize smart contracts.
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Summary of Findings</td>
</tr>
<tr>
<td>5</td>
<td>A Note about Terminology</td>
</tr>
<tr>
<td>6</td>
<td>About the Participants</td>
</tr>
<tr>
<td>7</td>
<td>Goals of the Pilot Program</td>
</tr>
<tr>
<td>9</td>
<td>Common Misconceptions/What a Recorder/Registrar Actually Is</td>
</tr>
<tr>
<td>12</td>
<td>The Recording Process in Cook County</td>
</tr>
<tr>
<td>15</td>
<td>What are “Blockchain” and Bitcoin?</td>
</tr>
<tr>
<td>17</td>
<td>Why Blockchain for Real Estate?</td>
</tr>
<tr>
<td>19</td>
<td>Why Blockchain for Government Land Records?</td>
</tr>
<tr>
<td>21</td>
<td>Theorizing Illinois’ First Legal Blockchain Conveyance</td>
</tr>
<tr>
<td>26</td>
<td>Blockchain and Cryptosystems at CCRD</td>
</tr>
<tr>
<td>31</td>
<td>Expansion on Summarized Findings</td>
</tr>
<tr>
<td>43</td>
<td>Conclusion</td>
</tr>
<tr>
<td>49</td>
<td>Sources and Works Consulted</td>
</tr>
</tbody>
</table>
Summary of Findings

The CCRD Blockchain Pilot Program produced a series of findings and results. These findings and this Report are the opinions of CCRD or the author alone, and should not be considered shared by Pilot participants.

Result: The participants designed a blockchain real estate conveyance software workflow that can be a framework for the first legal blockchain conveyance in Illinois (and possibly the US.)

Result: CCRD has successfully used components of blockchain technology (file hashing and Merkle trees) to secure government records on a site maintained by an authorized non-government reseller.

Result: CCRD used the concept of “oracles” to build the most informative property information website in Cook County, with a dedicated landing page for each parcel. These landing pages can be conceptualized as “digital property abstracts,” which help people see the benefits of consolidating important property information.

Result: CCRD’s current enterprise land records software vendor, Conduent (formerly Xerox/ACS) has agreed to incorporate some of the technology used in blockchains, particularly file hashing and data integrity certification, into the new land records system currently being installed at CCRD. Both parties will work together over the next year to explore further possible uses.

Below is a summary of CCRD’s findings and opinions. Each will be expanded further on in the Report, beginning on Page 31.

1. Blockchain technology is a known method for permanently storing transactional records that in a number of respects is superior to locally-isolated client-server models, and can provide a method of recordkeeping that is resistant to alteration, even by government officials.
2. The use of blockchain with a Proof of Work consensus algorithm that requires expending massive amounts of electricity to confirm each transaction is not ideal for real estate recordkeeping. Distributed ledgers may be a better option.

3. Blockchain can provide a mechanism to combine the act of conveyance and the act of providing notice (recordation) of the conveyance into one event.

4. “Blockchain” is not an all-or-nothing approach; aspects of the component technology can be implemented individually or selectively to improve recordkeeping outcomes.

5. Creating “Digital property abstracts” can consolidate property information that is currently spread across multiple government offices in one place, empowering residential and commercial property buyers, as well as lenders and other interested parties while creating a framework for a digital property token.

6. Protecting property conveyances with asymmetric key cryptography (akin to locking the transfer with a secret password), would make unauthorized conveyances more difficult, protecting homeowners and lienholders.

7. While digital signatures could phase out “wet” signatures from the public record and could thereby increase privacy and security, it could enable secrecy, and it remains important for Illinois’ land registry to remain open and continue to identify all who participate.

8. In many cases, a parcel could be easily conveyed using the Bitcoin (or another) blockchain, but if that process also included tokenizing title to the parcel and making the digital asset a bearer-asset; this further outcome may not be desired or, if desired, may create new challenges that must be addressed.

9. Separate from conveyancing, if the use of blockchain were to be extended to the maintenance of a records system, it would be most optimal if the record-keeping ledger were to be distributed across all land records offices in Illinois, allowing economies of scale and the ability to create true distributed consensus.

10. With the CCRD office slated for consolidation with the Cook County Clerk by 2020, it is not prudent to undertake any large conversion effort without knowing the commitment of the elected official who will ultimately run the combined office.
A Note about Terminology

Under current usage, the term “blockchain” can refer to a well-known, specific blockchain (the Bitcoin blockchain), a custom-built private or public blockchain, or the general idea of creating an immutable, chronological ledger of transactions protected against revision by encryption and consensus algorithms. Another common industry term is “DLT,” or “distributed ledger technology,” meant to differentiate databases built upon proprietary or custom ledgers, or those built without a “Proof of Work” algorithm or an associated cryptocurrency. CCRD is well aware that only very specific use cases truly can be considered a "blockchain."

This Report considers all forms of usage, and the author has made every effort to be clear in specific contexts to which blockchain is referenced. If a reference to a blockchain is not made clear, readers should envision a generic blockchain. The term “blockchain technology” generally means that certain attributes of a blockchain were utilized or packaged in a different way to achieve a desired result, but not necessarily in conjunction with a cryptocurrency or a widely-distributed consensus algorithm like “Proof of Work.” Perhaps the interchangeable term “cryptosystems” (coined by Ed Dunn¹) is more accurate than “blockchain technology,” but in the interest of consistency and furthering a conversation, common usage will be employed.

For this Pilot Program, the Bitcoin blockchain was selected by the conveyancing software company velox.RE because of its eight-year track record of immutability.

Throughout this document, the Office of the Cook County Recorder of Deeds will be referred to as CCRD.

¹ See: Dunn, Ed (Appendix)
About the Participants in the Pilot Program

**Cook County Recorder of Deeds** – Led by Karen A. Yarbrough since her election in 2012, CCRD is one of the largest land records offices in the United States. CCRD’s blockchain pilot efforts were led by John Mirkovic, Deputy Recorder of Communications and IT, with technical assistance provided by Don Guernsey of Onyx Electronics.

**International Blockchain Real Estate Association (IBREA)** – Founded in 2014, IBREA is one of the largest blockchain trade organizations in any sector (over 2,000 members), and is the leading organization applying the technology to real estate. IBREA helped develop and share knowledge, facilitated phone conferences, and served as a conduit for local informational updates and feedback. IBREA was founded by Ragnar Lifthrasir and is led by Noga Golan.

**velox.RE** – Orange County California-based technology startup founded by Ragnar Lifthrasir. velox.RE is a comprehensive real estate transaction and asset management platform built on Bitcoin blockchain and distributed file storage.

**Hogan Lovells** - Hogan Lovells, an international law firm with over 2,500 lawyers, including more than 800 partners operating out of more than 45 offices in the United States, Europe, Latin America, the Middle East, Africa, Asia and Australia. Hogan Lovells advised IBREA in connection with the Pilot Program. The Hogan Lovells team was led by New York-based partner, Lewis Cohen, who specializes in the application of blockchain and distributed ledger technology to complex financial, real estate and other transactions.

**Blockchain Consulting LLC** – Velox.RE was advised by Chuck Thompson, CEO and founder of Blockchain Consulting LLC. Chuck is also a member of the Board of Directors of IBREA.

**Goldberg Kohn** – CCRD was represented by Chicago-based pro bono counsel Goldberg Kohn, through its partners Gerald Jenkins and Gary Ruben, who assisted in legal research and reviewing this Report.
Goals of the Pilot Program

The overall goal of the Pilot Program, as stated in the press release announcing the effort, was to “test cross-compatibility between the client-server database model and distributed ledgers,” but also included a wide-ranging evaluation of the legal protections afforded to purely digital transactions. This was both a technological and legal inquiry meant to discern what types of transactions can be performed today, and how records that currently must necessarily be kept in two separate databases can be linked through a means acceptable to a Recorder of Deeds.

The Pilot Program, from CCRD’s perspective, was also initiated to learn how the process of conveying and recording real estate transactions could be improved via changes to state and local laws, and what specific laws can be adjusted to encourage electronic-only legal instruments.

A second aspect of the Pilot Program, initially focusing on approximately 2,000 vacant properties in Chicago slated for demolition, was meant to demonstrate how a “digital property abstract” could be created, and show how consolidating records held by multiple government offices across multiple layers of government will result in a holistic and accurate picture of the financial health of a property. Aggregating this data into one “location” is the first step to streamlining pre-conveyance due diligence, allowing the property title to transition from a sequence of scattered events to an actual “object” (the digital abstract). The term “abstract” is reminiscent of how records about a parcel of property have been kept in the past, and like the abstracts of the past, that the digital abstract could create an ongoing story of a property.

Additional aspects of the Pilot included:

- Test and analyze the statutory definition of a real property conveyance under Illinois law and whether a real property conveyance must occur on paper
- Test the concept of unification of conveyance and notice (i.e., making the act of conveyance and the updating of the public record a single event)
- Study how a real property conveyance can be made more private while still maintaining a level of disclosure that meets the public's needs

---

- Promote awareness of digital signatures
- Study the ramifications of locking property conveyances with asymmetric key pairs
- Promote awareness of blockchain and distributed ledger technology (DLT) amongst land records officials and lawmakers and ensure that government has a voice in the direction that conveyancing takes
- Demonstrate an open-minded approach that encourages Chicago, Cook County and Illinois to be leaders in this technology and to be “light-touch” regulators

It is also worth stating what this Pilot Program was not, which is necessary due to some media accounts that inferred more from the program than what was announced. This Pilot Program was not an effort to convert the current client-server database structure of CCRD to a blockchain structure. It was a study of technology and law, using a narrow data set. CCRD believes that converting its current public record, with over 190 million data points and 20 terabytes of images, would be a massive effort. With the office slated for consolidation with the Cook County Clerk by 2020, it is not prudent at this time to undertake such an effort without knowing the commitment of the elected official who will ultimately run the combined office.

These above-stated goals, unless otherwise stated, are those of CCRD.
Common Misconceptions and What a Recorder/Registrar Actually Is

Because we expect this Report to be read by many who are not real estate industry professionals, it is important to first establish a few baseline facts that should help to clear up some common misconceptions about what the public land record actually is. Additionally, the way land records are kept varies widely across the US and world, and this Section will help distinguish any practices or legal standards that may be different in Cook County and Illinois.

Because the complexity of guiding a real estate transaction from handshake to the closing table makes people reliant on intermediaries and legal experts, many homeowners are unsure or unaware of what a Recorder of Deeds office does, and what its purpose is. Further, many don’t know how they own their home (joint tenancy, tenants in common…), or even how to obtain a copy of the deed that proves their ownership. Some believe that they don’t own their home until after 30 years of mortgage payments. This reliance on third parties fosters unfamiliarity with property ownership and leads some to have incorrect assumptions about the role of CCRD and the purpose of a public registry.

A government land records office, such as a Recorder of Deeds, Registrar, or Clerk, is simply a place to provide public notice of land transactions and attendant encumbrances like liens (mortgages). The conveyance of a parcel of property from one party to another is effected by the use of a conveyancing document (typically, a type of deed), meeting the requirements of applicable law. Although they do not play a role in the actual conveyances or transactions, the public databases maintained by these elected officials serve a vital and fundamental role in the economy of the United States. Dr. Hernando De Soto, one of the world’s foremost researchers and scholars on private property rights, identified public land registries in his book The Mystery of Capital as the key to Western economic success, and stated that such a system is essential for developing nations to unlock the “dead capital” of their residents who cannot prove ownership of their own property.

The State of Illinois does not have a legal requirement that deeds and conveyancing instruments be recorded in a Recorder’s Office and, thus, recording a deed does not increase or enhance the validity of the conveyance. If properly executed, signed, accepted and witnessed, an unrecorded deed is just as “legal” (that is, enforceable by the buyer against the seller) as a recorded one.
Recording a deed does, however, provide valuable protections to the new owner. Because most financing contracts and mortgages require as a condition of borrowing money that the deed conveying the property and other associated documents be immediately recorded, as do the terms and conditions of a contract for title insurance, most deeds and conveyance instruments are recorded.

In Illinois, public information about real property is hard to find. Many are surprised that no single government agency has custody over all important data regarding real property and are often frustrated that they must visit so many different offices for necessary information relating to one transaction. Most are also not aware that a parcel of real property can be fraudulently conveyed to another by simply forging and recording a new deed, something that can be done anonymously through the mail.

Another misconception is certification of records. This action does not mean that the CCRD certifies that the legal claims made in recorded documents are true, but rather, that a physical reproduction of an instrument was generated from the Recorder’s master database and reflects a true and accurate copy of what was presented at the time and date stamped on the face. Certification is normally done with a physical embosser and can be confirmed via tactile inspection.

Under Illinois law, it is possible to possess an otherwise valid deed conveying property to the grantee, but the deed not being in a format entitled to be recorded. It is a common misconception that a Recorder of Deeds must accept all documents for recording. For example, if a deed does not display on the first page the information about who prepared it, it can be rejected for recording until rectified without affecting the validity of the act of conveyance described therein. If it is not in a physical format that allows CCRD to reproduce it, the document can be rejected.

Additional clarifications:

- Though a blockchain can increase privacy and anonymity, it can also increase secrecy, and it must be recognized that the U.S. economy has long been dependent on a public land record and upon everyone being able to engage with the owners of any parcel.
- In Illinois, new deeds are always created for subsequent transfers (a deed is not a bearer-asset).
- Unlike vehicle titles with a lien, the grantee receives the property deed (and ownership) upon acceptance of the conveyance. Even if there is a mortgage, the mortgage lender does not hold the deed pending complete satisfaction of the mortgage obligation.
- In Illinois, the Recorder does not have the authority to investigate legal claims made in documents, making it easy to commit property fraud. Because the land records system is open, it is possible to steal a property (on paper) by mailing in a forged transfer instrument.
- The Recorder is not the arbiter of who owns a parcel of real property. It keeps the public record that allows others to make that determination. Additionally, unrecorded documents may determine who actually owns a parcel.
- The Recorder of Deeds’ records are the only “official” records, and at this time, CCRD only accepts paper records, or scanned images of paper documents. This means that a blockchain transfer, to be afforded notice in Cook County, must ultimately produce a paper document that evidences a transaction.
- CCRD is not legally required to record everything presented to CCRD. It is from this principle that we derive our ultimate interest in the document that is presented for recording after a blockchain transfer. Many offices around the country, however, believe they must accept everything for recording.
The Recording Process in Cook County

Before fully understanding the role CCRD played in the Pilot Program’s test of blockchain technology, it is important to understand the role CCRD plays today in most real estate transactions.

Generally speaking, the Recorder of Deeds (in most jurisdictions) has no role in a property conveyance transaction, other than selling property transfer “stamps” (and collecting transfer taxes or fees) on behalf of the County and State. It is important to remember that the conveyance and recording are two separate acts, and as stated earlier, the act of recording is not required to have a valid conveyance. This means that the Recorder of Deeds is often the last step in the process, and the owners may take possession of the property even before the act of recording. This is because the conveyance already occurred upon signing and delivering the conveyance instrument.

Illinois’ public land records system is conceptually paper-based. Although it does not specifically require that deeds and instruments be on paper, the requirement that instruments be “in writing” is so easily satisfied with paper that it becomes hard for some to envision paperless transactions. Notarization (the process of having a trusted third party confirm the identity of the person signing a document) is also hard to accomplish on anything other than paper. Further, additional technological dependencies require that some physical representation of the conveyance be provided to the Recorder of Deeds, and the most obvious and efficient way to transmit this public data is bringing the original paper-based deed or other conveying instrument and having the Recorder’s office make a physical copy or replica. Though CCRD has taken steps to encourage paperless submissions (increasing paperless submissions from 185,000 per year to over 350,000), the hectic nature of closing real estate transactions leaves many industry professionals unable or unwilling to try new methods.

The storage and reproduction of public records throughout history has been limited to a handful of different formats, and is even mentioned in the Bible as consisting of creating two copies of a land deed (one sealed, one open, and storing them in earthenware jars - *Jeremiah* 32:9). Traditionally before 1924, conveying instruments and liens were brought to the CCRD and left there for employees to make complete transcriptions by hand into ledger books. Upon
completion, the original records were returned. CCRD then became, in 1924, the first recorder’s office in the country to use large overhead cameras to make facsimile reproductions of instruments. In the 1950s, the CCRD and many other recorder’s offices began using the more efficient method of microfilm and microfiche, a decision that at the time made sense but has proven to be a disaster as governments today struggle with the cost of converting those images to digital files because the film is deteriorating.

In the 1980s and 1990s, land records offices across the United States began transitioning to electronic database management systems (known as DBMS) that replaced ledger-book reproductions of documents with computer files created by scanning the original instruments, and replaced index books with computer databases. This era led to the adoption of electronic recording (“e-recording”), which is simply accepting documents for submission via an electronic method (e.g., a purchaser or their agent scans a paper document and then submits the image file to the recorder’s office electronically).

Though a document can arrive today at CCRD in one of three ways - over the counter (paper), mail or courier (paper), or e-recording (digital file) - the workflow for placing each of them in the public record is essentially the same. If a record is received over the counter, it is immediately scanned and converted to a digital computer file, and the original is immediately returned to the customer with a physical label placed on it indicating the time and date of receipt and its unique document number. The process is the same for documents received by mail, except that the original is returned via mail.

Before recording, each document submitted to the CCRD is reviewed for compliance with Illinois’ statutory basic recording requirements. If the document is deficient beyond the scope of a nonstandard penalty, it is rejected and must be adjusted or corrected before resubmitting. E-recordings must also meet the basic recording requirements, in addition to some technological attributes (high enough image resolution for clarity, 8.5” x 11” paper size, font size 10pt or larger, adequate margins). Electronic documents that are recorded are electronically returned to the customer with the recording timestamp electronically affixed.

All documents must then go through the next critical phase: indexing. Indexing a document is the manual extraction and keying of certain data points to enable searching and to allow the database
to render a full chain-of-title by displaying each document affecting a specific Property Index Number or PIN (the unique ID assigned to each parcel). Indexing the image file to the PIN and legal description is the fundamental way of keeping the public record organized, and mistakes in this process can make it impossible to find a document that represents a valid interest in or claim against property.

Therefore, the CCRD can be seen to actually keep two sets of public records: an image file of every document presented, and various indices (e.g., grantor-grantee index, tract index). The image record is the only record that can be certified by the CCRD; the index of data, while a helpful resource meant to enable people to locate a document using a variety of search queries, is by the nature of its creation subject to human error. It is believed that most title insurance companies do not rely on the data from the indices and generally inspect each image file themselves as needed to ensure accuracy.
What are “Blockchain” and Bitcoin?

Before understanding the potential impact of blockchain, it is important to understand how the first blockchain (Bitcoin’s) works in order to fully grasp why it is so revolutionary. Bitcoin is the world’s first true native Internet currency, meaning that it can be used in the way the Internet is used (peer-to-peer), can be used like cash and without a trusted third party intermediary to validate the transaction. The blockchain itself provides the settlement of the transaction and the notarization act of timestamping, while also ensuring the Bitcoin is not counterfeit.

For many years in the 1990s and 2000s, computer scientists and cryptographers could not implement an internet-native currency because there was no technology that could perform the role of a bank, and no technology to prevent the “double-spend” (or Byzantine Generals) problem. This meant there was no way to know whether the non-physical “money” sent to someone was genuine and not previously sent to someone else. By utilizing a shared ledger, where all users hold an identical copy of the entire history of every Bitcoin transaction, a ledger that reconciles across all copies every ten minutes (average), fraudulent transactions are not accepted by the blockchain, preventing a user from “giving” a single Bitcoin to multiple people (Bitcoins exist only as ledger entries; they are not “moved” in and out of separate accounts; rather, cryptography governs the ability to transfer control of Bitcoin to an intended recipient).

The blockchain is the underlying data management structure (database ledger) that makes Bitcoin possible. The Bitcoin blockchain was a novel and revolutionary idea whose genius comes from how it was assembled, as many of its components were not new at the time (2008-9). A blockchain is based on the concept of a distributed database (where all users share identical copies of the ledger), but one that not only can be read by all, but can be written to by all. “Blocks” are containers in which to package transactions, and they are “chained” together by linking the cryptographic hashes to the prior and subsequent blocks within each block. To insert a fraudulent transaction would require rewriting not only the block containing the transaction, but also at least every block that follows it.
Bitcoin protects itself against denial of service, spam and fraudulent transactions by using a protocol called Proof of Work, which ensures validity and consensus by requiring the expenditure of actual resources to solve complex cryptographic puzzles. This consensus is implemented by Bitcoin "miners." The miners are incented by the possibility of earning new Bitcoins, and their search for those new Bitcoins ensures the integrity of transactions on the Bitcoin blockchain. This process is the only way new bitcoin are created, and the protocol currently limits the total amount of bitcoin that can ever be created.

Mining bitcoin is a resource-intensive endeavor (electricity costs, component cooling costs), and the inventor(s) of Bitcoin utilized game theory to configure it, meaning that it is more profitable to participate in the system in the way it was designed (earning new bitcoin by helping ensure consensus) than it is to try to rewrite the transactions (it would cost more in electricity to attempt to manipulate the chain than it would to simply dedicate that computing power to mining for new bitcoin).

Though the Bitcoin blockchain is quite secure, private companies have been building their own enterprise ledgers using differing structures and consensus algorithms, or by creating an “altcoin” from the original Bitcoin code. Though there are many competing approaches as to how blockchain technology should be deployed, with partisans defending every side, CCRD has
identified some key components of the Bitcoin blockchain that should serve as minimum features of any custom-built blockchain or ledger that may be used by a governmental office:

- **Designed to be immutable** – This concept is commonly called “append-only” or “write-ahead-only” and ensures that existing records cannot be changed, but is realized only by technological enforcement through mathematical functions designed to be one-way (output cannot be used to derive value of input).

- **Distributed or shared** – Full copies of each individual office’s land records are stored by each office in the network, thereby automatically creating backups in multiple locations.

- **Non-repudiation** – An established and publicly accepted method of digitally signing transactions is used to self-certify acts, perhaps using official PKI standards, or a means for human notaries to attest electronically.

- **Designed to be autonomous** – CCRD is choosing to define autonomous here to mean that when the blockchain is deployed, significant coding effort is done up front to ensure that once it begins operation it cannot fail and thus cannot require constant or even routine maintenance. It should run automatically after data is fed into it and only in the way it was designed to work.

**Why Blockchain for Real Estate?**

If blockchain is thought to be a solution, it is important that we describe the problems it can solve.

It is hard to deny that the process of acquiring clear title to residential or commercial real estate is complicated, requiring the participation of many people, including the buyer and seller, lawyers for each, an escrow agent, an appraiser, a lender and their counsel (generally) and a title insurer. The process of acquiring clear title is sufficiently complicated that private insurance is usually obtained to cover any potential risks. However, as Goldman Sachs found in its 2016 report *Blockchain: Putting Theory into Practice*, title insurance may be the only type of
insurance where the cost of a policy is not based on actuarial risk (generally, miniscule, in dollar terms), but rather it is based on the actual labor and effort of title company employees.³

In response to the housing crisis of the late 2000s, where aspiration, greed and fraud combined to harm the global economy, the federal government began adding more regulations to an already highly-regulated industry sector. Though these reforms, specifically the combination of the Truth In Lending and Real Estate Settlement Procedures Act forms into one TILA-RESPA Integrated Disclosure (TRID) form, are meant to protect consumers by ensuring they “know before they owe,” the regulations also had the effect of making the closing process even more complicated and the outcomes more urgent and important. These reforms, in the author’s opinion, while well-intended and should end the closing-day surprises many are used to, have also made homebuyers even more dependent on “experts” such as attorneys and title searchers. This increased dependence in turn causes frustration for the general public, as they not only don’t know what is happening, but they also don’t know why or how.

Unfortunately, the increasing complexity and urgency described above will almost certainly create an environment that lends to mistakes, thus fueling a self-perpetuating system where title insurance is required to “cover” the new mistakes alongside the old ones. This increasing complexity, with many hands touching every part of a transaction, is not only the biggest challenge to implementing a new way of doing business, but it may also be the biggest reason for implementing a new way of doing business.

³ See: Goldman Sachs (Appendix)
Why Blockchain for Government Land Records?

Property records held by governmental entities are a natural fit with a database structure that technologically binds each record to its prior record. Under current retention conventions, documents on CCRD's land records website are displayed in reverse chronological order, with newest records on the top. Those who work in the property records industry already call the history of documents on a parcel a “chain-of-title,” making the comparison to a blockchain easy to understand. This chain-of-title is also legally immutable, meaning that records are never deleted, even if they were executed incorrectly by private parties.

These records are presumed to be unchanged by the general public who views them, and for nearly every record, that is the case. CCRD does not, as a policy, replace already-recorded document image files with new ones. In rare cases where an initial scan to capture the image by CCRD staff does not result in a clear image, the Quality Assurance process will re-scan the saved copy of the original submission, which is kept for 30 days.

Though the storage conventions show that blockchain makes sense for land records, it must solve a problem to make sense to move towards such a system. Problems currently experienced by government that could be addressed by this technology include:

Efficiency and Dwindling Resources: Government resources are scarce and mounting pension obligations are placing great pressure on the delivery of services. Blockchain can allow for improved service delivery using fewer employees, or it can enable a better service that will result in revenue for government and savings for homebuyers. It can also allow counties that lack the resources to implement electronic document recording systems to join an economy of scale. A system that is data-based rather than reliant on scanning documents and printing labels can be administered using standard desktop computers with fewer peripherals.

Accuracy: The current paper-dependent mode of executing and recording transactions requires (at CCRD) that a human employee manually inspect a scanned image of an instrument and retype the data points that are necessary for the property index to be searchable. This manual process is always at risk of error. These typing errors, combined with errors made by private parties in the preparation of the documents, create a near-accurate system and actually
perpetuates the complex and costly infrastructure needed to search and “clear” titles. As noted earlier, blockchains can unify the conveyance with the public record, meaning that the public record would be an exact and perfect replica of what actually happened, adding de facto accuracy to the de jure accuracy, or presumed accuracy, we have now.

**Security:** Though CCRD can assert that its current database is fully backed up in multiple offsite locations and that there has been no known breach of its records, CCRD cannot say that there is a mechanism to protect against what former NSA Director James Clapper calls “the next push of the envelope,” where malicious actors infiltrate systems like a Recorder of Deeds Office not to steal records, but to subtly and undetectably alter existing records, with the ultimate goal of eroding public and private-sector trust in government. Such a cyberattack, if successful, would shake the very core of our economic system and would exacerbate mistrust of government and business. A blockchain structure would make this type of attack far more difficult.

Although CCRD’s records are secure, that is not the case across the state of Illinois or across the country. Records have been lost in fires and database failures. Many offices do not have the resources to have redundant backups. Many offices do not even have electronic records and may be dependent on a physical means of storage like paper or microfilm. Blockchain may be the only database structure that is protected against manipulation by the very government stewards entrusted to maintain it. In some developing countries, blockchain is being studied and implemented for this very reason.

**Stagnancy:** When it comes to constructing and maintaining a public land record, the furthest that many counties (including Cook County) have advanced is the acceptance of scanned images of paper documents, including some that are a combination of type and handwriting. The first e-recording was accepted almost twenty years ago, and the document-submission industry is still trying to convert paper-only counties to this "new" technology. Blockchain-inspired technology provides an opportunity for government to self-identify the next generation of land records storage systems and participate in its adoption. For example, blockchain presents an opportunity to transition to a data-only records submission model, where only the key data points are stored as text.

---

Theorizing Illinois’ First Legal Blockchain Conveyance

The essence of a conveyance of property is information. To paraphrase (and reimagine) Marshal McLuhan’s famous aphorism “the medium is the message,” we must embrace the idea that in this case, the medium is *not* the message. The “message is the message,” meaning that the deed is not valid because it was on a piece of paper; it is valid because the information within it is clear and correct and that two people irrefutably agreed to it. Whether this message is transmitted on paper or via an electronically-signed and acknowledged event should not matter if we are to transition to paperless recordkeeping and transactions. What this also means is that we must start to think about a conveyance as simply an agreement, verifiable by a paper document or electronic file. Thus, the deed becomes what it really is – *information* – and not simply a piece of paper.

Through most of Illinois’ history, the only way to memorialize and convey information was paper. Though paper conveyances may be convenient, they are not the most secure, and because the conveyance and the updating of the public record are two steps under our current structure, a benefit of a blockchain conveyancing system is the ability to unify the conveyance with the updating of the public record. This future benefit may include making real estate transactions more efficient and more accurate, as the information that makes up the record is the very same information used in the conveyance.

Under today’s paper-based recording system, the information on the paper is retyped into a searchable database, which is how the public can find legal claims to a property. An error in retyping the Property Index Number means that unless another Grantor/Grantee name search is also performed, that claim may not be found and satisfied before a property is sold.

One of the main goals of this Pilot Program was to create a real-life scenario where a conveyance of real property can occur without a paper deed, while still satisfying the requirement that something that can be recorded into a county’s existing public recordkeeping structure also be produced. The ultimate purpose of recording an instrument is not to validate the conveyance or make the conveyance “more legal,” but instead is to provide notice to all, especially subsequent purchasers, that a certain person has a claim to the property. Though in the future the act of conveyance can happen within the public record, or simultaneously update the record, the
existing framework in Cook County and Illinois is such that the county government record is the only official record. This does not mean that an unrecorded, but otherwise valid, deed has no standing, but it does imply that a judge may not deem that an unrecorded conveyance nailed to the town square bulletin board provided sufficient notice to invalidate the claim of a subsequent purchaser. Without placing something in CCRD’s database, a blockchain transfer is no different than one nailed to a bulletin board.

Another goal of conceptualizing the first legal blockchain conveyance was to create a scenario where a legal conveyance happened without the need to record anything. This is due to the two-part nature of conveyancing and notice. The conveyance should be able to stand on its own; otherwise it carries no more weight than a verbal agreement or a vague chain of emails agreeing to convey a property. In this regard, it is important to note that CCRD does not endorse the practice of non-public conveyances. It is our position that a public record of all transactions involving each parcel of property is the most fundamental foundation of our economy, and according to De Soto, this public registry is the most important factor of economic success in the United States. Further, government (and the people) have an interest in knowing who owns a property not only for the normal practice of holding and owning property, but more importantly to address situations where the owner is failing its community, by, for example, not maintaining the property to the point it becomes a danger to others.

Taken together, to have the protections afforded by the law, some type of paper or electronic image in “perceivable” format must be submitted to the Recorder of Deeds Office in a format that meets current statutory recording requirements. Such a submission could contain very little information, but because the public record is meant to protect consumers, CCRD insisted through this process that the document that is ultimately recorded contains enough information to satisfy a public benefit of “who, what, when, where…” including metadata that allows the blockchain transaction to be located on its registry.

To satisfy this unavoidable need for a piece of paper, it was determined that a prudent course of action would be to have the buyer file with CCRD what is called a “Confirmation Deed.” This type of instrument is not common, but it is clearly referenced by the State of Illinois as being a
type of instrument exempt from transfer taxes (765 ILCS and 35 ILCS\(^5\)). That is because a Confirmation Deed is an instrument that is designed to be recorded with respect to a prior conveyance (the blockchain conveyance, in this case) with the purpose of clearing up any potential ambiguities in the prior deed. A Confirmation Deed was identified because of the extra layer of protection that it provides to the parties, which was important in this first-of-its-kind transaction.

**Summary of the Proposed Transaction Workflow**

It is not difficult to create a digital token, agree that it represents a certain asset, and transfer it between two people; but if it can also be said the transfer was structured in a way as to be a legal conveyance, then it would be noteworthy.

California-based startup velox.RE, as a participant in the Pilot Program, proposed building software based on open-source technology that allows two private parties to transfer digital assets without the need for a paper instrument. Velox chose the Colored Coins protocol, which is an information layer built over the Bitcoin blockchain that allows the creation of digital tokens to represent real-world assets, and those tokens to be transmitted with digital signatures, and that transaction tied permanently to the Bitcoin blockchain. Colored Coins also allows the tokens to be divided into smaller portions to represent shares of ownership. This protocol is also used by Nasdaq in their blockchain use cases.

Velox, CCRD, and participating attorneys spent months debating a theoretical software interface that would presumably meet Illinois’ threshold of legality for a conveyance. Under Illinois law, a conveyance or deed must generally identify who the parties are (grantor and grantee), provide a description of the property, have some explicit language “warranting” and/or “conveying” the property, identify a consideration amount, and be signed and dated. For the software to function correctly, these minimum public information points must be included in the plain-text metadata of the transaction, allowing both parties to digitally sign the conveyancing language, and any member of the public to read them.

---

For example, the conveyancing language that is signed would need a bit more information than is traditionally used on a paper deed, but is essentially the same, reducing a multi-page deed to one paragraph:

The Grantor, Bob A. Doe of Oak Park, Illinois, for and in consideration of one hundred thousand United States dollars, conveys and warrants to Grantee, Alice Q. Public, the following described real estate: PIN 12-34-567-890-0000 with the legal description of [INSERT TEXT or HASH OF LEGAL DESCRIPTION HERE], situated in the County of Cook, in the State of Illinois. The required property transfer tax declarations have been executed and filed via Declaration ID number 123456780. Dated December 19, 2016. Signed by Bob A. Doe with State of IL digital signature fs1d8df90979089 Signed Alice Q. Public with State of IL digital signature dfd767dfd7sdfs and witnessed by Marc A. Notary, a duly authorized notary public in the State of Illinois, commissioned until 2020, who inspected the photo identification of the grantor and grantee above, and affirms their identity and confirms their understanding that they intend to convey the property described herein in Illinois, and hereby electronically affixes his/her signature fdd43d6ds4trdd on December 19, 2016. The conveyance transaction instrument was prepared by Blockchain Legal, whose address is 123 Anyplace Street in Chicago, and when recorded, mail tax bill to 123 Anyplace Street, Chicago.

After the digital signing of the conveyancing language by both parties, the grantor (seller) would then transmit the Colored Coin representing the property to the grantee. Again, what would make this transaction unique is that the information or words needed to make the transaction a legal deed were digitally signed by the parties and included as plain-text in the metadata of the Colored Coins transaction.

It was also discussed that the software could encourage and incorporate the participation of a human notary. If the two parties are populating the information pertinent to the transaction on-screen in real time, the notary would be able to witness exactly what they are doing. Additionally, the information that is used to create the transaction is also populated in real-time to the Confirmation Deed, which is visible on the same computer screen. This would help the notary to understand what happened, allowing the notary to also inkstamp and sign the Confirmation Deed that prints at the end of the transaction and contains the necessary information to locate the transaction in the Bitcoin blockchain (such as block height and the transaction hash value.)
At this point, the recipient of the Colored Coin would be presumed to be the owner of the parcel being transferred, and he or she need not take any additional steps. He or she now controls the Colored Coin tied to the property and can now convey the property to another party using the same method. The word "presumed" is used because only a judge in a court of law can truly decide whether the conveyance was indeed legal, though CCRD believes that the totality of the evidence, the presence of the pertinent plain-text language within the metadata of the Colored Coin transaction, combined with the witnessing of a disinterested third party (notary), would make it difficult for the original grantor to successfully claim that they did not convey or did not intend to convey the property. The final step, recordation of the Confirmation Deed or a similar affidavit, is simply a common-sense act of insurance not meant to validate the transaction, but to protect the new owner against future claims.

Though much work was put into designing this software-based workflow, velox.RE ultimately chose not to perform a legal transaction in Cook County.
**Blockchain and Cryptosystems at CCRD**

Though much of the Pilot was an effort to design a conveyancing workflow and study the associated legal ramifications, CCRD looked at ways to incorporate aspects of this technology into its current operations.

**Background:**

*CCRD has been spearheading an effort in Cook County to crack down on illegal ‘contract-for-deed’ scams where fraudsters sell homes that cannot be acquired or occupied to unwitting buyers. One of the main reasons the buyers become victims is that they were unaware that they needed to check multiple government offices to learn if the property could be acquired.*

**Goals of CCRD Efforts:**

- *Use blockchain technology in a way that provides value (not an invented use case)*
- *Test the creation of digital property abstracts and demonstrate the value of consolidating property data*
- *Secure official records on a third-party (non-government) website and enhance their reputability*

One commonly-known use of the Bitcoin blockchain is as a timestamp ledger that can certify the existence of a specific computer file at a point in time. This is done by creating a SHA 256 hash (digital fingerprint) of the file, then using the bitcoin OP_RETURN function to permanently embed a hexadecimal translation of that hash into the Bitcoin blockchain by marking it as an unspent transaction. This would be useful if a Recorder of Deeds did lose their entire land records image database. If a customer had the digital file they originally submitted and also submitted it to the blockchain, they could prove that it matches this blockchain record, in essence using another public database to certify records.

Currently such a service exists – ProofOfExistence.com. CCRD did test this service and found that it (or a similar feature) could be incorporated into future land records software, but the per-transaction fee (approximately $4 per record) made it very expensive and not worth utilizing on a scale larger than a simple verification test.
During the Pilot Program, a need to protect the integrity of CCRD records arose. The Office entered into a contractual relationship with Onyx Electronics for the purpose of reselling document images to “power users,” those who want an easier-to-use and more powerful software interface than currently provided by CCRD’s official 20/20 PerfectVision software. It became clear that blockchain-inspired technology could be used to certify the integrity of not only the files hosted on this third-party site, but also that the chain-of-title for each property could be hashed and those values used to detect any irregularities or changes in the records.

The Onyx site also, in light of CCRD’s desire to create digital property abstracts to empower those who might be deceived into buying condemned homes, became a test environment that could be customized, where the soon-to-be replaced PerfectVision software could not be modified.

The first step in creating CCRD Onyx was to copy all existing records (190 million, 20 TB) to Onyx’s servers. The TIFF images were converted to PDF, all pages watermarked for security, and the images were realigned to the indexing data, which was organized in a way to make searching faster and easier. This process took three months.

After all the records and data were transferred, Onyx began plugging in “oracles” (trusted data sources) to build the digital property abstracts for each parcel. Though it was initially mentioned that CCRD would do this for properties on the Chicago Demolition List, these abstracts were able to be created for every parcel in the County for which we could find information. In addition to each parcel’s chain-of-title (chronological history of recordings), the following information was added directly from their source:

- the photo of the property (Assessor)
- tax assessment attributes, such as lot size and square footage (Assessor)
- property tax payment and appeal history (Treasurer)
- GIS satellite map (County Clerk)
- Google Map (Google)
- Chicago building permits and violations (City of Chicago)
- latitude and longitude satellite coordinates (US Census)
From this consolidated information, a new data visualization was created, called Property Health. Property Health allows interested investors or aspiring homeowners to see at a glance any issues that may prevent them from acquiring the property. Rather than overwhelming the user with data, the new visualization uses simple yes/no logic and color coding (red/green) to indicate whether a property may have worrisome characteristics.

For example, if a property has been sold for unpaid taxes, is or was subject to Chicago building code violations, has or had legal actions such as foreclosures, or appears on the Chicago Demolition List, the Green box would show Red, letting the individual know that the property has been flagged and more research should be done.

Once all the relevant data and oracles were implemented, the next step was to implement the SHA 256 hashing of records and construction of Merkle trees for each parcel. This process first involved the creation of three SHA 256 hash values for each document: one for the Property Index Number (PIN), one for the combined document number and recording date, and a hash of
certain document image file metadata. The three hashes are then hashed together into a digest for each record. The process is repeated for each document in the chain-of-title, and the digests for each document are then hashed together to create a final Merkle root for each parcel. What results is a flagging mechanism that will alert CCRD and any public viewer if some record has been manipulated, and this flag would be triggered if any of the four genesis points has been changed. This single Merkle root value could be certified in the Bitcoin blockchain as well.

Figure 4: Screenshot of public-facing SHA 256 Merkle tree on CCrecorder.org

A Merkle tree is a mathematical construction used in Bitcoin and elsewhere to certify the validity of each transaction within a block of transactions and to ensure that none of the individual transactions within the block has been manipulated. The Merkle root creation also allows large volumes of data to be validated without having to examine each transaction. By imagining each recorded document as a transaction or block, each property’s transaction history can be conceptualized as an individual “blockchain.”

The Onyx software then provides a certification date for the Merkle root of each property, which provides researchers with a date and time certain upon which subsequent requests for the same data can be compared. If, for example, a hacker inserted a fake mortgage or deleted a document from that property’s chain-of-title, the hashing operation would recognize that the Merkle tree has been compromised and let the viewer know this fact. If a new document with even one pixel changed is substituted, the Merkle tree would break. As each new document is recorded on the property, the Merkle root is updated and certified with a new date.
CCRD and Onyx recognize that this usage of blockchain technology is a “cryptosystem” and not a blockchain. However, the creation of digital property abstracts and the public-facing certification of file integrity using SHA 256 shows a path forward for the next generation of land records management technology and how adopting this technology need not be an all-or-nothing approach. In fact, CCRD’s current enterprise land records software vendor has agreed that this technology should be a standard feature on their new AgileFlow Records Manager.

To be taken directly to a parcel’s hash-verification page, visit:

http://ccrecorder.org/parcels/show/parcel_bc/1000000/
Expansion on Summarized Findings

1. Blockchain technology is a known method for permanently storing transactional records that in a number of respects can be superior to locally-isolated client-server models and can provide a method of recordkeeping that is resistant to alteration, even by government officials.

Prior to commencing the Pilot Program, CCRD extensively studied the blockchain technology behind Bitcoin and determined that it was successfully open-sourced, tested, and had been safely operational for eight years. Given that the current market cap of Bitcoin approaches $30 billion, there exists sufficient motivation to find and exploit any weaknesses in its construction. Unlike other competing blockchains like Ethereum, the Bitcoin blockchain has not been exploited. Any known or reported “hacks” of Bitcoin, like Mt. Gox in 2014, were actually hacks of third party software “wallets” meant to store the private keys that must be kept secret and not a hack of the Bitcoin blockchain itself.

Contrary to popular belief, most hacks or breaches of records don’t involve weaknesses in technology, but weaknesses in people. Social engineering, for example, is much more effective in gaining access to protected systems than brute-force attacks. Because blockchain records are resistant to manipulation, even by the government officials charged with maintaining them, the technology is becoming popular as a method of reform and data integrity in the developing world.

Under U.S. law, the public record of property transactions is afforded de jure immutability, meaning it is presumed to be immutable without actually being immutable. Blockchain would make the public record more difficult to change and could, therefore, introduce de facto immutability. Implementing a truly irreversible record is not only a major step forward for technology and security, it sends a strong message that the government is interested in true reform.

Blockchain’s immutability can make it superior to a central client-server. In a true blockchain storage system, every record that would need to be stored by any office would be stored by every office. For example, every Clerk/Recorder office in Illinois could be a node in a blockchain or...
distributed ledger network and digitally sign off on the veracity of other office’s records. Such a distributed system would make loss of records virtually impossible, which in that respect makes distributed ledgers superior to using a centralized server. Once records are permanently secured, implementing records retention policies becomes an easy effort.

With recent news about the potential of Bitcoin becoming two separate blockchains, caution should be exercised when considering that a single registry built upon Bitcoin could exist in two blockchains, creating confusion about which is the true record. Further, having two almost identical blockchains could pose risk of a “replay attack,” where transactions sent on one chain are intercepted and reused to make identical transactions on the other.

It must also be noted that Bitcoin’s blockchain is not actually immutable as a system. As Dr. Gideon Greenspan pointed out in a recent article⁶, a nation-state with a goal to destroy Bitcoin could do so for less than a billion dollars. They could accomplish this by writing their own version of the Bitcoin blockchain that meets the longest chain test (and most Proof of Work). Miners may then unwittingly begin to create new blocks on the fake blockchain. Once the attack was revealed, the value of Bitcoin would likely plunge to zero, and any records pegged to Bitcoin transactions using models like Colored Coins would likely be rendered dubious at best.

In a sense, if Bitcoin survives, it will be because of the people dedicated to updating and maintaining the Bitcoin codebase, not the codebase itself. As seen recently with the threat of a forced hard fork of the ledger into two, some leading developers are recommending changing Bitcoin’s Proof of Work algorithm to prevent this, and thus potentially removing the hashpower now held by centralized mining farms using free or subsidized electricity to gain a computing power advantage.

2. *The use of blockchain with a Proof of Work consensus algorithm that requires expending massive amounts of electricity to confirm each transaction is not ideal for real estate recordkeeping. Distributed ledgers may be a better option.*

---

⁶ See: Greenspan, Gideon (Appendix: The Blockchain Immutability Myth)
Bitcoin’s blockchain is secure and immutable because of its unique Proof of Work algorithm. This type of security is necessary for a completely decentralized, anonymous and peer-to-peer transaction system. This type of consensus generation is also useful for creating general decentralized systems.

Real estate, however, is not in need of the type of decentralization required for Bitcoin. Just because one could build an anonymous peer-to-peer system for exchanging tokens they have agreed to represent real property, does not mean that one should. Most Americans depend on an open and public land records system that is kept by a single authority. This is how they can borrow money to purchase a home and tap their equity to send their children to college. A future where people are instantly and anonymously trading real estate may make sense to technologists, but its impact on our economy must be studied before heading in that direction.

What can be decentralized in real estate is the ability to submit a public record. In this regard, blockchain and DLT, if implemented alongside consolidated records and data-only records submission, can be seen as a path towards a real estate system that regular people can understand and use, one where they are not reliant on paying thousands of dollars to those who can interpret the confusing nature of how property records are kept.

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

Mining Bitcoin can be conceptualized as turning electricity into currency. Conservative estimates of the amount of electricity needed to mine one Bitcoin at “5,500 kilowatt-hours - half the annual consumption of an average U.S. household.”7 Twelve and a half Bitcoin are created through

---

mining roughly every ten minutes. There are arguments to be made that a wholesale switch by large industry sectors such as banking to a Proof of Work validation structure would save enough money in other costs to make the increased energy consumption a wash, but the environmental impact must be understood and considered, especially for recordkeeping that is not an intensive bricks-and-mortar resource commitment.

Though the Bitcoin blockchain is the best current method for transacting value and allowing unknown parties to reach consensus, distributed ledgers may be more efficient for keeping public records that are not created in a peer-to-peer manner. This does not mean that in the future that permissioned and permissionless blockchains could not be linked.

3. **Blockchain can provide a mechanism to combine the act of conveyance and the act of providing notice (recording) of the conveyance into one event.**

When one purchases a home, it is a two-step process to ensure that purchase is protected. Step one is ensuring that the conveyance by deed was completed correctly. The second step is placing a record of that transaction in the official government registry. In Cook County and Illinois, the second step is effectuated by manually retying information from the scanned document into an index that makes it searchable by the public. This manual process undoubtedly subjects the public record to a level of error that would be eliminated by unifying the conveyance and the creation of the public record.

If the process were consolidated, the only errors that would be present in the public record would be errors created by the public before the conveyance. This is how the public land record is supposed to work, as it should be an exact reflection of what is contained in the instrument. Further, by unifying the conveyance and the creation of the record, risk of pending claims that aren’t indexed prior to a transaction (but are still valid claims nonetheless) is mitigated, as the record populates much faster, closer to “real time.” Regardless of implementation, it makes sense to explore new ways of creating public land records, including data-only or data-first submission.
4. “Blockchain” is not an all-or-nothing approach; aspects of the component technology can be implemented individually or selectively to improve recordkeeping outcomes.

The Bitcoin blockchain itself is not a single piece of technology; it is a combination of already-existing technologies such as digital signatures, asymmetric key cryptography, distributed ledgers, and peer-to-peer communication. Additionally, though Bitcoin has been in uninterrupted usage since 2009, almost all the original code from the pseudonymous and anonymous creator(s) “Satoshi Nakamoto” has been replaced. Though Bitcoin does require all the pieces of the puzzle be in place for it to work, keeping land records does not require an “all-or-nothing” approach. While it makes sense to put all similar offices in a state or region onto a shared and distributed ledger, individual offices can implement single-office private blockchain ledgers to replace their “unchained” index database.

Additionally, much like CCRD/Onyx did in implementing a hashing technology cryptosystem, there are aspects of blockchain technology that can be implemented on limited budgets. This is especially valuable to governments that may have limited resources or that wish to test certain use cases. Though CCRD prefers to wait until full-stack solutions are better developed and participation from more Illinois counties, it is supportive of the idea of individual offices implementing aspects of cryptosystem technology, and in fact, will be doing so with its current enterprise software vendor, Conduent.

5. Creating “Digital property abstracts” can consolidate property information that is currently spread across multiple government offices in one place, empowering residential and commercial property buyers, as well as lenders and other interested parties while creating a framework for a digital property token.

One of the biggest problems with transacting real estate is that the information required for pre-sale due diligence is spread across different government agencies, as well as local and state government.

Selling a used car is a relatively straightforward transaction, whereas selling a property is, at best, a complex, legal saga. While it is estimated by Goldman Sachs that 30% of property titles
are not “clean” and have deficiencies, even the transfer of property without title issues is a complicated endeavor involving many people. One thing that makes vehicles easier to convey than houses is that there is not a large amount of research that must be done before buying the car. If the buyer physically has the paper title and the seller’s name matches the seller’s ID, the transaction is a simple matter, and the buyer need not consult multiple government agencies. In buying a house, relevant information affecting one’s ability to acquire a certain property exists in at least five offices, including the Recorder of Deeds, Assessor, Treasurer, Circuit Court, City of Chicago, as well as consultation of GIS plat maps held by the Clerk.

This decentralization of information is what, in CCRD’s opinion, leads people to depend upon expensive experts to help navigate this process. This reliance on others also results in a general unfamiliarity of what is needed to buy a property, and when people are not empowered with information or understanding, they are unable to make good decisions. For example, many aren’t aware that title insurance does not protect them against fraudulent claims on their property made after they acquire it.

The problem with decentralized data has become very clear in Chicago’s ongoing problem with scammers selling blighted homes as ‘contract-for-deed’ to persons who lack the resources and credit history to qualify for a bank mortgage. While in the right scenario, buying a house in very poor shape and rehabbing it can be a great way to acquire a home or start a property investing business, it is a risky endeavor if the buyer is unaware of what he or she should be looking for and where to look. For example, CCRD has encountered victims of a fraudster who sells properties he does not even own (sometimes outright, sometimes as “contract for deed”), many of which are barred from reconveyance by a judge due to their very dangerous condition. Additionally, many of these homes have delinquent utilities and water bills which must be paid before a deed can be recorded. In some cases, the amount of past due utilities and taxes equals or exceeds the value of the property, and these victims do not have the resources to come up with another $20,000. In some extreme circumstances, victims pay the fraudster $15,000-20,000 in cash, spend thousands of dollars of their own money on renovations, only to find that they cannot record the deed and assume ownership.
Before starting a public education campaign on what to look out for when purchasing blighted, low-value properties, CCRD felt that it is important to first create a place where all this information should be housed. Knowing that CCRD’s official public records portal (PerfectVision system) lacked the functionality to handle such a task, including the ability to search for properties by address, it was decided that the Onyx Site would best host this information. Once CCRD/Onyx was built, SHA 256 technology was used to secure the integrity of the files on the site, meaning CCRD can now tell the public that research done on Onyx is as accurate as research done on 20/20, and the hashing technology can help set time/date baselines to monitor the integrity of a chain-of-title. CCRD believes that this public-facing hashing technology should be built into all next-generation Land Records Management Systems (LRMS).

Before the Internet and digital technology, it was hard to conceptualize a property transfer as an easy task, primarily because the required information seemed almost purposefully hidden. Digital property abstracts are an important step towards building a blockchain-based property conveyance structure, and an important step towards helping people understand how real estate actually works in the United States.

6. Protecting property conveyances with asymmetric key cryptography (akin to locking the transfer with a secret password), would make unauthorized conveyances more difficult, protecting homeowners and lienholders.

Property fraud, which can consist of fraudulent conveyances or false and frivolous liens, has been one of the fastest growing white-collar crimes since the housing crash. CCRD has encountered hundreds of people over the last four years who are victims of this crime. The fact that a home can be easily conveyed illegally with paper is one of the reasons CCRD began exploring this technology.

One simple way to demonstrate how blockchain technology can create an immediate and recognizable improvement to the way real estate is conveyed is to use the example of Wi-Fi and passwords. Most Cook County residents own smartphones. Most residents have some sort of online account that requires a password. When people learn that it may be easier for their
neighbor to steal their home than it is to steal their Wi-Fi, they start to grasp the security benefits blockchain provides.

Asymmetric key cryptography is accomplished by creating key-pairs (a public key and private key) that are mathematically related, as opposed to creating a single decryption key that must be securely transmitted to the entity you wish to share information with. The public key can be thought of like an email address. It can be shared with anyone, and in fact, must be shared with the person you wish to give or receive value from. The private key is analogous to a secret password and must be kept secret and secure.

Under current law and our paper-based system, a fraudster could create a fake deed using graphic design software, find the owner’s signature on a prior public record like a mortgage, and create a new deed that appears as if the owner sold or gave their house to the fraudster. At this point, the scammer need only to mail it in to CCRD and pay the recording fee (approximately $50). If the property has no liens, like a mortgage, the fraudster could then use their “paper ownership” to strip the equity, rent the home to others, or sell it. If property conveyances were allowed only upon the entry of a public and private key, the unauthorized transfer of a property would be almost impossible. Even if the fraudster were able to hack or coerce the private key from the owner, the very fact that the transfer must happen on a computer makes it harder to cover one’s tracks than is possible using U.S. mail.

In addition to protecting homeowners from unauthorized conveyances, lenders would also be protected from fraudulent releases of mortgage, much like a bank prevents the unauthorized sale of a vehicle it loaned money against by physically holding the title. Blockchain, through the use of multi-signature technology, allows the creation of automated legal agreements (smart contracts) that can automate back-office tasks like the verification and filing of a satisfaction of mortgage.

7. While digital signatures could phase out all “wet” signatures from the public record and could thereby increase privacy and security, it could also enable secrecy, and it remains important for Illinois’ land registry to be open and identify all who participate.
CCRD believes that digital signature technology, a key component of blockchain, has existed long enough to have proven itself as a viable means to eliminate the need to hand-sign most documents. Therefore, a goal of this Pilot Program was to raise awareness of digital signatures and show how they can be more secure than wet signatures and how they can provide a more durable and immutable record of who signed what and when. Because scammers can use a signature found on CCRD’s website to commit further fraud with banks, landlords, etc., digital signatures can and perhaps should be more widely used.

Though these signatures can increase privacy, a fundamental aspect of the public land registry must be the clear identification of who is participating, noting that Illinois does still have a land trust system that can provide a layer of identity protection while still maintaining regulations that allow the owners to be identified when a legal need arises. As stated earlier, the service of identity verification is now performed by a notary, and will likely remain an important defense against repudiation. Some in the blockchain land records space see the technology as a way to transition to a system of anonymous property transfers, but CCRD believes such an approach undermines what De Soto identified as one of our strongest economic assets, our public land record. One idea that deserves further study is how blockchain can allow a layered approach to privacy, keeping personal information away from potential scammers while still allowing that information to be accessible either by those in law enforcement who need it, or if the owner of the data approves it.

8. *In many cases, a parcel could be easily conveyed using the Bitcoin (or another) blockchain, but if that process also included tokenizing title to the parcel and making the digital token a bearer-asset, this further outcome may not be desired or, if desired, may create new challenges that must be addressed.*

The Bitcoin blockchain was designed to be very good at keeping track of a limited amount of data. But, as the widely-respected Nick Szabo said, “…the limits of Bitcoin’s language and its tiny memory mean it can’t be used for most other fiduciary applications.” ⁸ Upgrades like the

---

⁸ See: Szabo, Nick. [https://unenumerated.blogspot.com/2014/12/](https://unenumerated.blogspot.com/2014/12/)
OP_RETURN unspent transaction feature in 2014 did allow small amounts of data to be encoded into the blockchain, but not in plain text. A public land registry, on the other hand, requires a larger amount of information to be stored, and to be stored in a “perceivable” format.

The Colored Coins protocol is used to add more functionality to the blockchain by creating a token to represent an asset, which is under the control of private keys, the same as Bitcoin. This process, however, can make an electronic deed a bearer-asset (property that is deemed owned by the person possessing it, not because it is licensed in a registry), like cash. If the owner of the property loses the private key or it is stolen from his or her computer by a hacker, the property token could be conveyed to an anonymous public address. Such a possibility requires the development of special protocols to safeguard keys, including the usage of multi-signature transactions or escrow services to hold keys. Additionally, some legal process would need to be created to apply for a “lost key,” similar to the lost title process for a car. Though the idea of preventing the conveyance of a property with a password may be better than the current system where anyone can file a forged piece of paper, CCRD believes that more people may lose their private keys than currently have their homes illegally conveyed, especially because Bitcoin private keys are very long and complicated (such as 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF) and cannot be chosen or memorized by the user. This issue needs further study.

Under Illinois’ current property and recording system, a deed is not a bearer-asset. When a property is sold, a new deed is created, rather than adding the new owner’s name to a master title. Keeping a record of a property’s history using a token on a blockchain necessarily requires that same token be reused. Further complications exist such as dividing ownership and thus, dividing tokens, and what to do when a parcel is split into two or more new parcels. These are all concerns that could be solved, but they do show how the use of blockchain can change the very nature of property ownership and conveyance.

9. Separate from conveyancing, if the use of blockchain were to be extended to the maintenance of a records system, it would be most optimal if the record-keeping ledger
were to be distributed across all land records offices in Illinois, allowing economies of scale and the ability to create true distributed consensus.

Though it would be possible to now implement some form of blockchain storage structure for existing and future land records, CCRD believes the opportunity is most fully realized through a wide-scale participation, allowing all Recorders to work together to add, store and verify records. For this reason, CCRD will continue to work through existing channels, such as the Illinois Blockchain Initiative and the Illinois General Assembly Blockchain and Distributed Ledger Task Force (authorizing legislation pending approval⁹), to explore ways to encourage a transition to this more robust, secure and accurate means of storing public records. Putting time and work in these areas will allow the industry to focus on the shared needs of all Recorders, and build a digital infrastructure that will serve these needs in an all-in-one package, as opposed to layers of existing software pinned to a blockchain that is controlled by unaccountable entities.

Further, by encouraging a collaborative path forward, the State of Illinois can bring a truly modern and fully paperless records management system to parts of the state that may not be able to afford custom software and hardware. If planned correctly, such digital infrastructure can be used for multiple areas of government recordkeeping beyond land titles, such as vehicle titles and university transcripts.

10. With the CCRD office slated for consolidation with the Cook County Clerk by 2020, it is not prudent to undertake any implementation effort without knowing the commitment of the elected official who will ultimately run the combined office. Upon consolidation, it could make even more sense to pursue a blockchain database that can be used both for land records and election records.

A challenge to the future of blockchain and distributed ledger efforts at CCRD came a few weeks after the announcement of the Pilot Program. The voters of Cook County were given the deciding vote in whether CCRD would be consolidated into the County Clerk’s Office, like most

counties in Illinois, and voted to merge the offices. The question was raised as to how this decision to consolidate would affect the Pilot Program, and the answer is that it makes the opportunities more important, because the impetus of the consolidation was cost savings. Regardless of the path chosen, the ultimate decision should still rest with the new Cook County Clerk in 2019.
Conclusion

The Cook County Recorder of Deeds (CCRD) has a history of leading the recording industry in technological adoption. In 1924, CCRD became the first county in the US to use overhead cameras to make reproductions of documents. CCRD’s history has also been fundamentally shaped by one of the worst disasters in our region’s history, the Great Chicago Fire of 1871. This event not only saw many public records lost, but placed the financial security of Cook County in the hands of both the public and private sectors, as government (for a period of time) was dependent on private records kept by Chicago Title and Trust\(^{10}\). This relationship, in a way, characterizes the entire land records industry – an amalgamation of complexity and interdependency that is self-perpetuating.

What Should Come First?

Because it is easy to misunderstand how real estate is transferred and how that information is made public, it is easy to let one’s imagination run wild and believe that blockchain or DLT for land records could be implemented overnight.

Though blockchain can make transacting real estate simpler, safer, more accurate and easier to understand, there are challenges facing its adoption. In many cases, these challenges are the very reasons why such a new structure should be adopted, and thus can also be looked at as opportunities.

One of the biggest challenges may be resisting the urge to remake our nation’s real estate system to fit a blockchain. It is perhaps more innovative to see how we can use technology to change legal processes rather than to first change legal processes so that they can fit a specific technology. For example, the impacts of making real estate instruments into bearer-assets (tokens) need further study and input from legal experts.

Before a blockchain or DLT system can be developed statewide in Illinois, some legal and structural changes must be considered. Should we first consider requiring all legal claims to a property to be placed in the public record? Should we continue to spread vital property

\(^{10}\) See: http://www.ctic.com/history.aspx
information across more than five government offices? Should we continue to maintain a property records system that is different in each county, or make an effort to standardize the data or format?

*Figure 5: Bitcoin transaction detail showing complexity of information*

Blockchain and DLT represent a great opportunity to improve the transactional nature of real estate, but it would be a shame if we also did not use the opportunity to implement changes that make it easier to understand how real estate is transacted. For example, for a statewide real property records system to make sense, the public record should be stripped down to plain-text data inputs, and perhaps a permanent hash value of the sales contract file. Such an effort would make public records more lightweight, more accurate, and more importantly, they would be standardized and look nearly the same across the entire state. We need look only to our neighbor, Iowa, to see what a push towards standardization would do for the people of Illinois: “Iowa uses a highly standardized system for documenting property records, and it maintains a shared online database where county records can be easily accessed from anywhere in the state,” and as perhaps the only state that fully guarantees citizens against title defects, its “… loss rates are the lowest in any state, as less than 2% of premiums are paid to settle claims.”

---

11 See: Goldman Sachs (Appendix)
By first standardizing data and parcel-numbering formats and relieving taxpayers of the burden of visiting more than five government agencies to learn about a property, we can then explore ways to use this empowerment to make it easier for two individuals (with the same set of information) to trade real estate between them. We can explore ways to make it easier for a roofing contractor to file a lien with his smartphone, rather than needing to leave the jobsite to visit his lawyer, then drive to a Recorder’s Office to hand-file it. We can explore ways for software providers to offer innovative new user interfaces utilizing the standardized data and digital infrastructure of a distributed ledger.

**Why Should Government Care?**

Though the United States has one of the best real estate systems in the world, it would be unimaginative to not consider how blockchain and DLT technology can make it better. Our system sometimes seems held together by sheer willpower and the large sums of money that flow into America’s title insurance industry. With over 30% of land titles having defects and even a title insurance executive admitting in a recent blockchain whitepaper\(^\text{12}\) that fraud is rampant in real estate, we can see a need to pursue a public record that is safer, more accurate, and more easily understandable.

Fraudulent property transfers are one of the main reasons CCRD became interested in blockchain, and the idea that conveyances could be protected behind a password. At a recent CCRD community event, a member of the audience, upon learning how easy it is to steal property in our paper-based system, asked why she has to enter a password for all aspects of her financial life, but not this most important event? The public is beginning to ask for this technology, even if they don’t what to call it.

Highlighting the problems facing the industry is not to meant to suggest that title companies do not provide a useful service. In fact, they are the glue that holds most real estate transactions together. Their hard work, in most cases, results in a smooth transaction and clear title.

Blockchain technology not only represents an opportunity to create better outcomes for taxpayers, it’s an opportunity for elected land records officials to shape the conversation. Much

---

\(^{12}\) See: Spielman, Avi (Appendix)
like the technology behind MERS cut the public land registry out of an opportunity to provide more public information, the development of this technology represents a risk to government officials who do not participate in its adoption. Some believe that a distributed ledger or blockchain can replace government record-keepers. While it is hard to say whether this will ever happen, government probably won’t be replaced by a database whose creators are unknown, and whose future is in debate.

What’s Next for CCRD?

As stated earlier in this paper, CCRD is not interested in a ‘go it alone’ approach. As Bitcoin developer Jeff Garzik stated recently in remarks noting that private, permissioned blockchains will be the path to public ones: “Blockchains are networks, and a network of one is not very exciting.”

We will continue to work with the Illinois Blockchain Initiative and the Illinois General Assembly to study state-specific opportunities and challenges, and to promote Illinois as a leader in this new technology. For example, though we believe blockchain (paperless) conveyances are legal under Illinois law, perhaps the statutes can be modified to provide affirmative authorizations that mention immutable registries. Illinois could also look at making remote notarization by video legal, as it can better help automate transactions while providing an even more durable record of an event resistant to repudiation. Developing standards for allowing technology to self-certify records, and studying the legality of smart contracts are also an opportunity for lawmakers.

CCRD will also continue to work with technology partners who share our interest in finding a distributed ledger structure that makes sense for government. In future efforts, we will work with the industry to develop future-case functionality and towards a stronger and more logical public land record.

The CCRD Blockchain Pilot Program unfolded alongside (and in many ways shaped) the national conversation on blockchain technology, and for that reason the conversation shifted in

---

many ways. For example, Ethereum’s hard fork into two separate ledgers in mid-2016 appeared to show that Bitcoin’s blockchain would be the technology to survive, but new fears in early 2017 about Bitcoin becoming two separate ledgers and currencies, or the very heart of the code (the Proof of Work algorithm) being completely changed, show that there is still time to study the question as to which type of blockchain or distributed ledger is the best choice for a long-term government records project.

Despite the fact that the first legal blockchain conveyance was not performed, the Pilot resulted in a clearer path forward for blockchain and DLT efforts in Illinois. More importantly, it resulted in a sense that there is still time to develop the right technology, as well as the right environment in which to encourage development of that technology. As Paul Van Valkenburgh of Coin Center said, “…all new approaches to decentralized computing – whether closed or open – should be celebrated and allowed to develop relatively unfettered by regulatory or government policy choices.” 14 This statement also makes it incumbent on those who want to work with government to develop these technologies to be open to working with blockchains and distributed ledgers, and to build with a clear solution, not just the technological capabilities, in mind.

Just as “blockchain” isn’t the answer to every problem, decentralization isn’t always the answer either, especially if the process it attempts to reform is not in need of it in the first place. Proof of Work for the Bitcoin blockchain is very resource intensive and expensive, and the entire real estate process need not be restructured in order to fit it to the way the Bitcoin blockchain works. Improving the way real estate is transacted also does not need be tied to people using Bitcoin to buy real estate.

When communication does not need to be peer-to-peer (recording a document is one person communicating with one government office, not any person anywhere), other validation methods can be explored. Consensus in land records can be a validation that the data was submitted in accordance with the pre-set rules, and was submitted via an approved method (from an approved office, or from a government-built web application). Again, Van Valkenburgh: “Closed systems may be the smarter choice for limited rather than general purpose decentralized computing tasks,

14 See: Van Valkenburgh (Appendix)
where consensus need not be open to all potential participants and participants can be centrally identified and trusted not to collude against the interests of the group.” 15

Also, if the outcomes are not urgent, then the consensus can be relaxed. For Bitcoin, the consensus must be as strong and decentralized as possible because the outcome of its irreversible nature is that an error will mean that one person will not have money they were expecting. In land records, so long as the deed is not a bearer-asset, an error is not life-changing; a new instrument can be created to rectify the situation. A house will not disappear before an error can be corrected. A land conveyance is not irreversible in law. There is still time and plenty of new ideas worth considering, ideas like the Distributed Byzantine Fault Tolerance (dBFT) algorithm used by distributed ledgers like Hyperledger, that allows consensus to be reached without the possibility that the ledger can be split into two by users.

There are very compelling reasons that blockchain and distributed ledgers are a natural fit for keeping land records and streamlining the dozens of intermediate steps needed just to get a deed into the public record. Real estate records are already kept in an immutable chain format by government. Most recorders, registrars and clerks currently keep these records not only in a chronological chain for each parcel of property, but in a timestamped chain of all records received with references to previous records. This existing structure makes it easier for decision-makers to visualize a cryptographically-secured computerized chaining structure for land records, and the transition to such a system.

Make no mistake, a transition from the status quo to a blockchain-powered real estate industry will require a lot of work and education, but the payoff appears to be worth the effort. If the national conversation around blockchain real estate plays out as some think, we could see new industry workflows centered around liquidity, accuracy, immutability and efficiency. As some developing nations have recognized, a blockchain bedrock is what you would use if you were creating a land records system from scratch. For that reason alone, it’s worth striving for in the United States.

# # #

15 ibid
Works Consulted or Cited

Below is a list of papers, articles and publications that were read, analyzed, or otherwise referenced in this Report.


Assia, Yonan; Buterin, Vitalik; Hakim, Lior; Rosenfeld, Meni, Lev, Rotem – *Colored Coins Whitepaper*. (2013)


Goldman Sachs – *Blockchain: Putting Theory into Practice*. (Schneider, Blotstein, et al, 2016)

Greenspan, Dr. Gideon – *MutliChain Private Blockchain White Paper– Coin Sciences* (July 2016 revision)

Greenspan, Dr. Gideon – *The Blockchain Immutability Myth*. Published on CoinDesk.com (May 9, 2017)


Torpey, Kyle - *Bloq: Private Blockchains are the Training Wheels for Enterprise Adoption of Bitcoin and Ethereum*. Published on cryptoinsider.com (April 13, 2017)

