Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues
About Perkins Coie’s Blockchain Industry Group

Perkins Coie features the world's largest and leading Blockchain Technology & Digital Currency industry group because we were here when it all began. Our firm started advising clients about tokenization and bitcoin, and has since expanded to helping our clients pioneer numerous and diverse uses of blockchain technology.

LEADER, NOT A FOLLOWER

Established in May 2013, this industry group represents more of an evolution than a genesis. As part of the greater Electronic Financial Services group, Perkins Coie has a long history representing technology companies that provide consumer and financial services, including mobile payment providers, tokenized in-game assets, e-commerce companies, and marketplace payment service providers. Naturally, when the first bitcoin and other decentralized virtual currency companies emerged, Perkins Coie was uniquely situated to launch an industry group focused specifically on blockchain technology and digital currency that now has over 40 lawyers advising clients across a range of issues. This group has helped more than 200 clients reconcile complex regulatory compliance questions, assess intellectual property opportunities, negotiate with regulators, and educate the greater population about the promises of blockchain technology.

WE ARE HELPING SHAPE THE INDUSTRY

Our team participates as observers to the Uniform Law Commission Study Committee in its drafting of a model Regulation of Virtual Currency Businesses Act. We work closely with Coin Center, The Chamber of Digital Commerce, and the Bitcoin Foundation, the world’s leading trade associations representing the digital asset and blockchain industry. We are founding participants in many industry and academic initiatives including COALA’s Blockchain Workshops, The Digital Assets Accounting Consortium, The Berkman Klein Center for Internet & Society’s Blockchain Roundtables, The Smart Contracts Alliance, and the DC Blockchain Center.

YOUR LEGAL PARTNER IN INNOVATION

Our multidisciplinary group is on the front lines, helping clients address the complex legal issues faced by bitcoin and other virtual currency businesses and partnering with those who are pioneering new blockchain and other distributed ledger solutions to many of today’s market challenges. We provide regulatory compliance counseling, litigation support, consumer protection counseling, and business transaction assistance for a range of bitcoin and digital currency systems, services, and products. Our clients include virtual currency exchanges, blockchain innovators both large and small, payment processors, investors, and industry associations.

We counsel virtual currency industry clients with respect to various regulatory issues, including compliance with the Bank Secrecy Act, FinCEN regulations, and securities and commodities laws and regulations. We help them draft anti-money laundering policies and organize their internal policies and practices for compliance. We have also assisted these clients in the face of inquiries and investigations by federal and state law enforcement and regulatory agencies. Our experienced Investigations and White Collar Defense group regularly defends corporate clients and individuals against criminal and civil allegations of fraud, money laundering, and other misconduct. Our defense practice includes particular experience in defending clients and property against government asset seizures and forfeitures.
# Table of Contents

## INTRODUCTION

**I. A (VERY) BRIEF INTRODUCTION TO SMART CONTRACTS**

THE ORIGINS OF SMART CONTRACTS

SMART CONTRACTS IN A DISTRIBUTED LEDGER TECHNOLOGY WORLD

**II. A REVIEW OF THE CURRENT ACADEMIC AND INDUSTRY LITERATURE ON SMART CONTRACTS**

SMART CONTRACTS AND CONTRACT LAW

TECHNICAL DIFFICULTY POSED BY SMART CONTRACT DEVELOPMENT

EMERGING USE CASES TOUCH UPON ENTIRELY DIFFERENT LEGAL REGIMES

**III. EXPLORING THE LEGAL ASPECTS OF SMART CONTRACT APPLICATIONS**

SMART CONTRACTS IN CAPITAL MARKETS AND VENTURE CAPITAL

SMART CONTRACTS FOR SUPPLY CHAIN MANAGEMENT

SMART RECORDS FOR GOVERNMENT AND SMART CITIES

SMART CONTRACTS FOR REAL ESTATE REGISTRIES

SMART CONTRACTS FOR ENABLING SELF-SOVEREIGN IDENTITY

**IV. AN INITIAL RISK MITIGATION CHECKLIST FOR BUSINESSES DEVELOPING SMART CONTRACTS APPLICATIONS**
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 discussion of the legal implications of those use cases that are unrelated to contract law. To fill that gap, this white paper offers an initial analysis of the legal aspects of five prominent smart contract use cases: capital markets and venture capital, supply chain management, smart government records and smart cities, real estate land registries, and self-sovereign identity. We conclude that legal risk is inherent in each of these subject areas, but that with careful risk mitigation planning, companies can overcome those hurdles to offer effective products and services.

This white paper proceeds in four parts. Part I briefly 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 explain the importance of smart contracts for businesses and lawyers. Part III introduces five uses of smart contract 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 when launching a product or service that uses smart contracts to mitigate legal risk.

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. ¹ 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 contact 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 computerized transaction protocol that executes terms of a contract." ² Szabo’s original idea of smart contracts was broad enough “that he considered ‘digital cash protocols’ to be a ‘fine example of smart contracts.’” ³ Szabo’s idea lay dormant for many years because the technology did not yet exist to support the implementation of smart contracts. ⁴ Then, in 2009, the Bitcoin blockchain emerged—itself a limited form of a smart contract. ⁵ Later, Ethereum offered 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. ⁶ 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 NICK SZABO, SMART CONTRACTS (1994).
⁵ Reyes, supra note 3, at 15; RICHARD GENDAL BROWN, A SIMPLE MODEL FOR SMART CONTRACTS, (Feb. 10, 2015), http://gendal.me/2015/02/10/a-simple-model-for-smart-contracts/.
SMART CONTRACTS IN A DISTRIBUTED LEDGER TECHNOLOGY WORLD

The Bitcoin blockchain, Ethereum, and other similar software protocols which we refer to broadly in this white paper as Distributed Ledger Technology (“DLT”), reigned 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, permanent transaction management system maintained through a consensus mechanism rather than by a trusted third-party intermediary, and that guarantees execution.”7 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 being used in academic literature and among standard-setting bodies as the broadest term, covering the Bitcoin blockchain, the Ripple protocol, Ethereum, and others.8 Further, DLT is broad enough to capture emerging platforms such as R3’s Corda. DLT also encompasses both proprietary (permissioned) DLT9 and open source (permissionless)10 DLT11. 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 upon 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.”12 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.”13 The Bitcoin blockchain itself is a smart contract with the limited purpose of executing transactions that involve the exchange of assets.14 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.”15

---

7 Reyes, supra note 3, at 9 (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 Walsh, The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, 18 NYU J. LEGISLATION & PUB. POL’Y 837, 840 & 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, distributed 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 in so far as the concept necessarily means the protocol is not as decentralized as the permissionless originals, 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 8-9 & nn. 24, 27.
12 TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 312 (2014).
13 MOUGAYAR, supra note 6.
14 BROWN, supra note 5, at 2.
15 HENNING DIEDRICH, ETHEREUM 67 (2017). “Ethereum has its focus on smart contacts 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 DLT;
- 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, smart contracts will modify other data;
- External data can be supplied by “oracles”—trusted data sources that send information to smart contracts (not all smart contracts require 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”;
- Smart contracts can track changes in state over time;
- Smart contracts are not the same thing as Ricardian contracts, which are “semantic representations that can track the liability of an actual agreement between parties”;
- 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;
- Once operating, 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;”
- Smart contracts are distributed because they exist as software running on a DLT protocol that itself is distributed across a variety of network nodes; and
- Smart contracts guarantee execution of the contemplated transaction.

Clearly, smart contracts offer the capacity to revolutionize any number of traditional processes, including those we discuss in further detail below. 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 from academics and legal professionals regarding smart contracts.
II. A REVIEW OF THE CURRENT ACADEMIC AND INDUSTRY LITERATURE ON SMART CONTRACTS

To date, most of the discussion among both attorneys and academics regarding smart contracts 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. Finally, we use this literature review as an opportunity to 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 analysis applying law to smart contracts centers on contract law. Such analysis focuses on smart contracts in a narrower sense than described above, centering on "a spectrum of possibilities for smart contracts, ranging from contracts that merely automate implementation or performance of natural language contracts (e.g., the release of payments under a natural language contract) to contracts entirely written in code." In other words, most existing legal analysis focuses 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 make execution of a legal agreement automatic, as merely a new form of self-help that fits rather neatly within existing contract law. As a result, most of the literature considering smart contracts 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." Authors also predict that conducting legal contracts through smart contracting computer code can bring clarity, predictability, auditability, and ease of enforcement to contractual relations. Such analysis of smart contracts as varying forms of legal contracts offer both useful and productive insights into the changing legal landscape. As the discussion below will demonstrate, however, many of the use cases for smart contracts currently do not involve implementing the terms of legal contracts through computer code. Rather, current use cases often offer software as a service, similar to existing business models. The difference, of course, is that the software is DLT-based and incorporates smart contract functionality. This white paper offers the first initial consideration 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 that correctly coding smart contracts to do what the software developer intends can be more difficult than programing traditional software. Furthermore, the self-executing nature of DLT causes even small errors to have significant effects. For example, the Ethereum-based decentralized...
autonomous organization, commonly referred to as “The DAO,” operated pursuant to smart contracting computer code. The code contained a known bug (that programmers were actively working to fix) which ultimately allowed one 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, is an Ethereum veteran with a university degree in theoretical and mathematical physics. He is not a seasoned coder or software system architect. But he is a smart guy who understands Ethereum. He even had professional experience as a software tester. In other words, even well-educated computer scientists with experience in the field and a deep understanding of Ethereum can make mistakes when programming with smart contracts. “That even he can trip up, predicts that a lot of people trying their hands at smart contracts will.” In fact, because of the difficulty of coding smart contracts, the 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 liability relating to mistakes in programming. Such legal issues may include product liability, breach of (the software as a service) contract, unfair and deceptive trade practices, and cybersecurity, among others.

EMERGING USE CASES TOUCH UPON 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 four such use cases, explain how smart contracts make them possible, and provide an introductory discussion of the applicable legal regimes.

III. EXPLORING THE LEGAL ASPECTS OF SMART CONTRACT APPLICATIONS

This section explores four emerging uses of smart contracts: real estate registries, smart government records, supply chain management, 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 will arise as projects in each area become more prominent and more frequent.

SMART CONTRACTS IN CAPITAL MARKETS AND VENTURE CAPITAL

How Are Smart Contracts Used in Capital Markets and Venture Capital?

The potential uses of smart contracts applications in capital markets and venture include syndicated loans, cash equities, collateral tracing, leveraged loan trading, fundraising through token sales for tokenized goods and services, and tokenized securities. One of the more developed use cases lies in the realm of cash equities. 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 process.” Goldman Sachs envisions smart contracts used to “eliminate[] duplicative confirmation/affirmation steps, shrink[] the settlement cycle, and reduce[] trading risk, which in turn should lower the industry’s cost and capital needs.” In total, Goldman Sachs estimates that the use of smart contracts in these ways could result in approximately two billion dollars in cost savings could be achieved in the U.S. alone, with approximately six billion

34 “The DAO is the name of a particular DAO, conceived of and programmed by the team behind German startup Slock.it—a company building ‘smart locks’ that let people share their things (cars, boats, apartments) in a decentralized version of Airbnb.” David Siegel, Understanding the DAO Attack, COINDESK (June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists/. Generally speaking, however, “A DAO is a Decentralized Autonomous Organization. Its goal is to codify the rules and decision-making apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control.” Id.
35 Id.
36 DIEDRICH, supra note 15, at 54.
37 Id.
The use of smart contracts for token sales related to tokenized goods and services continues to grow. Many DLT protocols, including the Bitcoin blockchain and Ethereum, depend on intrinsic tokens (e.g., bitcoin and ether, respectively). The tokens encourage users to validate transactions, impose minor transaction costs that prevent spam but do not discourage legitimate activity, and give the token-holder the right to participate in the network. Recently, many companies combined the sale of such tokens with smart contracts to create a form of democratized venture capital. In fact, many such companies enjoyed venture capital success through DLT token sales. In 2016, around 65 major token sales, when taken together, raised over $225 million. The average amount of funds raised in a single token sale was $1.6 million, while the median amount raised was $500,000. The token sales rely on smart contracts, frequently built upon the Ethereum protocol because of its more sophisticated smart contract capabilities. Ultimately, these sales blur the line between tokenized goods and services and tokenized financial returns, which, in turn, creates novel legal issues to assess. A second, but related trend relates to formally using smart contracts and tokens in venture capital. In broad terms, “[t]he Ethereum smart contract says, ‘I’m investing one bitcoin’—let’s say it’s worth $1,000—‘and at the end of the crowdsale I get $1,000 worth of that token.’ The smart contract is actually doing the issuance of the token to the investor. Instead of having the [chief financial officer] send you share certificates, the smart contract is sending you tokens that are representing the security in that company.” Overly using smart contracts for venture capital in this way allows regulators and participants alike to draw much clearer lines around how to treat the activity. The novel legal issues presented by both trends are detailed below.

Legal Aspects of Using Smart Contracts in Capital Markets and Venture Capital

We first consider the legal issues raised by token sales. From a legal perspective, even though token sales are usually 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. 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 with the expectation of profits, (ii) in a common enterprise, and (iii) 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, for most token sales, the investment of money and common enterprise prongs are often satisfied because to purchase a token you make an investment of money, and there is generally a promise of financial return for the investment. As a result, the expectation of profits and efforts of others elements of the test are often pivotal in the token sale context. Because the Howey test is so fact dependent, the outcome for any given token sale may be different.

As to the second trend, actors pursuing the issuance of tokenized securities generally seek to leverage the token sale trend to sell what is clearly recognized as a security by everyone involved. For example, the venture capital firm Blockchain Capital is seeking 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. In order to ensure that the sale is conducted in compliance with current regulations, the sale is being conducted by an entity incorporated in Singapore, where the Monetary Authority of Singapore’s 2014 guidance on token sales provides needed clarity. Blockchain Capital is using the Regulation S and D exemptions with the Securities and Exchange Commission to allow the sale to raise money from international and domestic investors. In doing so, Blockchain Capital offers an example to companies that the venture capital firm hopes to finance in the future, thereby mitigating the firm’s risk as a fiduciary of the money belonging to others by financing only regulatory-compliant deals. In so doing, even though Blockchain Capital is the first to admit it is offering a security for sale, the first to require know-your-customer compliance, and the first token sale used in the context of a fund, the fund’s general partner is betting that its work will pave the way for a new wave of token sales in 2017.

**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.” 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. Today’s economy involves a new type of supply chain—one that is more fragmented, more complicated, and more geographically diffuse. “In effect, the supply chain is now an opaque and faulty process that is extremely hard to manage.”

As a result, neither intermediate buyers nor the ultimate consumers are able to reliably confirm the value of the goods and services they purchase. 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. 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.

---

52 Eha, supra note 45.
53 Id.
54 Id.
55 Id.
56 Ben Dickson, Blockchain has the potential to revolutionize the supply chain, TECHCRUNCH (Nov. 24, 2016), https://techcrunch.com/2016/11/24/blockchain-has-the-potential-to-revolutionize-the-supply-chain/.
57 Id.
58 Id.
59 Id.
60 Id.
61 Id.
DLT protocols can operate as “a distributed, single source of shared truth.” Layer on top of that shared, trusted source of truth the capacity of smart contracts to update the state of the transaction in real time or to “trigger events that can be used to indicate the success or failure of a transaction,” and many routine difficulties in supply chain management can be significantly mitigated. 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 and to prevent fraud and enhance capacity for accurate freight audits.

In one implementation of this idea, a service “enables every physical product to come 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 uninterrupted chain of custody from the raw materials to the end sale.”

**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 upon all publicly held companies. Additionally, the California Transparency in Supply Chains Act imposes obligations upon entities that “do business” in California and have annual sales of $100 million or more. Furthermore, companies importing or exporting products across boarders 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.

---

64 Id.
66 Id.
67 Id.
70 Id.
71 Id. For other services in the supply chain space, see Blockverify, which is trying to provide a simple way to verify the authenticity of medicine, Everledger, which is trying to bring transparency to the diamond supply chain, and Kouvola Innovation, which seeks to provide a smart tendering solution for the supply chain.
SMART RECORDS FOR GOVERNMENT AND SMART CITIES

What Role do Smart Contracts Play in Smart Government Records and Smart Cities?

Reports of governments investigating the use of recordkeeping systems deployed on the blockchain abound; such governments include the United Kingdom,73 Estonia,74 Dubai,75 the U.S. federal government,76 and various state governments in the United States (e.g., Vermont,77 Delaware,78 and Illinois79). Some government interest can be attributed to a belief in DLT’s capacity “to vastly reduce the cost and complexity of getting things done.”80 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.”81 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.82 Possibilities for revamping the U.S. personal property filing system used to record secured transactions conducted under Article 9 of the Uniform Commercial Code, and for making Bank Secrecy Act compliance less burdensome have also been suggested.83 In fact, the European Union is presently exploring DLT’s potential to lessen compliance burdens in the financial services industry.84

In a 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.85 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.”86 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.”87 In the realm of benefits and entitlements, Illinois hopes to leverage DLT to reduce fraud and allow more efficient distribution while also increasing transparency.88 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

78 Giulio Prisco, Delaware Blockchain Initiative to Streamline Record-Keeping for Private Companies, BITCOIN MAG. (May 9, 2016), https://bitcoinmagazine.com/articles/delaware-blockchain-initiative-to-streamline-record-keeping-for-private-companies-1462812187/.
81 Prisco, supra note 78.
83 Reyes, supra note 3.
84 DIEDRICH, supra note 15.
85 HOLLOWAY, supra note 79.
86 Id. at 5.
87 Id.
88 Id. at 6.
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 start-up 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 in capital markets. Since its launch of this effort in October 2016, Dubai has launched the Smart Dubai Office Blockchain Challenge in partnership with global accelerator 1176, launched its own Smart Dubai Accelerator at the Dubai Future Accelerators, and announced initial contract awards for IBM and Consensys. By all accounts, Dubai’s plans for smart government record keeping 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 upon 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 record-keeping 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 record keeping may raise important questions of administrative law. 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 and/or undesirable decision? Who will be at fault if the code executes prematurely because it misread the circumstances?” Although the administrative law burdens will fall to the state agencies embarking upon 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.” As a result, those businesses offering software-as-a-service solutions

---

89 Id.
90 Statement attributed to His Highness Sheikh Hamdan bin Mohammed Al Maktoum from a speech made on the launch of the Dubai Blockchain Strategy, October 5, 2016, in “Smart Dubai: Dubai Blockchain Roadmap” (slide deck on file with authors).
91 “Smart Dubai: Dubai Blockchain Roadmap” at 7 (slide deck on file with authors).
92 Id. at 12.
93 Id. at 13.
95 Carpenter & Hughes, supra note 82.
96 Reyes, supra note 3, at 41.
97 Id. at 43.
98 Id. at 44 (citing FRANK PASQUALE, THE BLACK BOX SOCIETY 110-113 (2015)).
to governments seeking to implement a smart records regime must remain vigilant and cognizant of laws relating to antidiscriminatory 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.” 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. 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.” Without proper title, an enabling mechanism for leveraging assets, the assets held by the poor members of developing nations are “dead capital,” 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.

*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.” 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.” 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.

---

100 Id. at 5–6.
101 Id. at 6.
102 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).
Greece has also expressed interest in developing a blockchain-based land registry; in Greece “only 7% of the territory is adequately mapped.”\(^{106}\) 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.\(^{107}\) 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.\(^{108}\) 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.\(^{109}\)

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).”\(^{110}\)

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.\(^{111}\)

### 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.\(^{112}\) 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.\(^{113}\) 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.

---

106 Blockchains, supra note 97.
112 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.
113 For an in-depth consideration of how to undertake such considerations, see Reyes, supra note 3.
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 like Facebook and Google 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 (e.g., Facebook Connect). 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 their online identity with a host of other providers.\(^\text{114}\)

In this context, an ideal form of digital identity has been described as 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—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.\(^\text{115}\) 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.\(^\text{116}\)

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. 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.

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 a business to rely solely upon 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 Billey Act, and the Securities Exchange Commission’s Regulation S-P mandate that personal


\(^{116}\) TOBIN & REED, supra note 114, at 9.

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.\footnote{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, \textit{Death and Privacy in the Digital Age}, 94 N.C. L. REV. 927 (2016).}

Further, to the extent that financial institutions rely upon 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 if 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.

\section*{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:

\begin{itemize}
  \item What is the legal context in which the smart contract application will operate?
  \item 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?
  \item 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?
  \item What hazards are posed by use of the smart contract application alone?
  \item What hazards are posed by using the smart contract application with other software?
  \item Are there hazards that should be designed or guarded against?
  \item What warnings or instructions are necessary and/or advisable?
  \item Where and how should the warnings be displayed to limit liability exposure if the application malfunctions?
  \item 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?
  \item What contractual provisions do you need to limit liability and maximize the availability of indemnification?
  \item Have you considered and properly contracted around issues unique in the software-as-a-service context?
  \item Have you considered and properly contracted for software code audit services?
  \item What privacy and security law considerations do you need to bake into the smart contract application?
\end{itemize}