Smart Contracts: 12 Use Cases for Business & Beyond

A Technology, Legal & Regulatory Introduction — Foreword by Nick Szabo

Prepared by: Smart Contracts Alliance — In collaboration with Deloitte

An industry initiative of the Chamber of Digital Commerce

CHAMBER OF DIGITAL COMMERCE

December 2016

About the Chamber of Digital Commerce

The Chamber of Digital Commerce is the world's largest trade association representing the digital asset and blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain-based technologies. Through education, advocacy and working closely with policymakers, regulatory agencies and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs and investment.

Contact

Chamber of Digital Commerce
1133 15th Street, NW, 12th Floor
Washington, D.C. 20005
policy@digitalchamber.org
+1-202-765-3105

Table of Contents

Foreword
by Nick Szabo

It is exciting to see my vision for smart contracts, that I conceived over 20 years ago, blossom into so many different and creative directions. Evolution toward smart contracts would be inevitable even if the concept did not exist. Financial companies have, since I first explored these ideas in the 1990s, already implemented what are effectively smart contracts without using that phrase.

As much as smart phones are more functional than traditional phones, which in turn are in many ways more functional than messages written on paper, smart contracts can be more functional than their inanimate paper-based ancestors. Smart contracts can automate many different kinds of processes and operations, most obviously payment and actions conditional on payment. For example, making control of collateral dependent on whether a debtor has chosen to pay a loan on time – the fundamental logic here is automating “if-this-then-that” on a self-executing basis with finality.

The humble vending machine is the original form of a smart contract. At its core, a vending machine is a security mechanism: the amount in the till should be less than the cost of breaching the till. Additionally, the machinery reflects the nature of the deal: it computes and dispenses change as well as the customer’s choice of product. Today the most secure environments for smart contracts are the most mature public blockchains, which are designed for trust minimization instead of trusting the often private and insecure system found resident with a central party.

Many of the smart contracts proposed or described in this paper, or elsewhere, are meant to operate between large institutions, or between institutions and their customers. The smart contract goes beyond enterprise business solutions – in fact my personal favorite and most exciting type of smart contract is constructed in peer-to-peer environments, from simple natural language by individuals to operate between individuals. This movie will get even more exciting when machine-to-machine adoption takes shape at the intersection of blockchain, artificial intelligence and the Internet of Things.

Smart contracts involve objectively verifiable performances, or performances that can be automated such as cash flows. As a result, financial contracts, broadly and creatively defined, present obvious opportunities. Smart contracts can reduce the costs of people having to calculate complicated outcomes, and thereby make possible new kinds of contracts that weren’t possible before. Contracts-for-difference, are an example where software very rapidly and continually adjusts balances and can dispense cash flows based on frequently updated market prices. Smart contracts — by minimizing the need to trust a counterparty, a third party, or a foreign legal system — can also reduce counterparty risk and expand credit and other contracting opportunities through such trust-shifting technology.

Blockchain technology appears very much to be the jet fuel necessary for smart contracts to become commonplace in business transactions and beyond. It is a delight to be part of a community committed to fostering the tenants of open source cooperation, privacy and security, education in technology and working for a common social good.

Acknowledgements

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their thought leadership, oversight and support to the Smart Contracts Alliance, and the production of this white paper:

Smart Contracts Alliance Leadership

Lewis Cohen
Partner
Hogan Lovells LLP

John Jacobs
Executive Director
Georgetown University Center for Financial Markets and Policy

Matthew Roszak
Co-Founder & Chairman, Bloq
Chairman, Chamber of Digital Commerce

Alan Cohn
Of Counsel
Steptoe & Johnson LLP

Caitlin Long
President and Chairman
Symbiont

Mark Smith
Co-Founder & CEO
Symbiont

Jerry Cuomo
IBM Fellow and VP of Blockchain Technologies
IBM

Joseph Lubin
Founder
ConsenSys

Ronald Smith
Partner
Norton Rose Fulbright

Jeff Garzik
Co-Founder & CEO
Bloq

Sean Murphy
Partner
Norton Rose Fulbright

Margo Tank
Partner
BuckleySandler LLP

Marley Gray
Principal Program Manager, Azure Blockchain Engineering
Microsoft

James Newsome, Ph.D.
Founding Partner
Delta Strategy Group

Lata Varghese
Assistant Vice President, Blockchain Consulting Practice Leader
Cognizant

J. Dax Hansen
Partner
Perkins Coie LLP

Eric Piscini
Global FSI Blockchain Leader
Deloitte

Mark Wetjen
Global Head of Public Policy
Depository Trust & Clearing Corporation

Thomas Hardjono
Chief Technology Officer
MIT Connection Science

Jim Regan
President & CEO
Digital Federal Credit Union (DCU)

Micah Winkelspecht
Founder & CEO
GEM

Acknowledgements

The Chamber of Digital Commerce would also like to thank the following individuals and organizations for their valuable contributions to the Smart Contracts Alliance, and the production of this white paper:

Subject Matter Experts

Bertrand Alexis
Attorney
Harvard Law School

Edgard Alvarez
Counsel
Hogan Lovells LLP

Griffin Anderson
Head of Blockchain Accounting
ConsenSys

James J. Angel, Ph.D.
Associate Professor, Georgetown University Center for Financial Markets and Policy

Marc Aronson
President & CEO
Pennsylvania Association of Notaries

Judd Bagley
Director of Communications
Overstock.com & t0.com

Brian Blaha
Partner
Wipfli LLP

Preston Byrne
COO & General Counsel
Monax

Michael Chodos
General Counsel, Senior VP
Notarize

Tom Ding
Co-Founder & CEO
String Labs

Harry Gardner
EVP, eStrategies
Docutech

Rashi Goyal
Manager, Blockchain Consulting
Cognizant

Rouven Heck
Product Lead - Digital Identity
ConsenSys

Christine Ing
Partner
Blake, Cassels & Graydon LLP

Jordan Kruger
Data Scientist
Bloq

Mark Ladd
VP, Industry & Regulatory Affairs
Simplifile

Christian Lundqvist
Decentralization
ConsenSys

Scott Mehlman
CEO
Orebits.io

Thessy Mehrain
UX & Product Strategy
ConsenSys

Jerry L. Miller
Partner
Wipfli LLP

Theodore Mlynar
Partner
Hogan Lovells LLP

Jennifer Peve
Co-head Office of FinTech Strategy
Depository Trust & Clearing Corporation

Carla Reyes
Bruce R. Jacobs Visiting Assistant Professor of Law
Stetson University College of Law

Yorke Rhodes
Global Business Strategist / Blockchain & Identity
Microsoft

Michael Ross
President
Paragon Public Relations LLC

Sue Ross
Senior Counsel
Norton Rose Fulbright

Ira J. Schaefer
Partner
Hogan Lovells LLP

Michael Sena
Product Manager
ConsenSys

Jacqueline Shinfield
Partner
Blake, Cassels & Graydon LLP

Michael Sinclair
Consultant
Norton Rose Fulbright

Dana Syracuse
Senior Counsel
Perkins Coie LLP

Manish Tomer
Director, Blockchain Consulting
Cognizant

C. Richard Triola
CEO
NotaryCam, Inc.

R. David Whitaker
Senior Counsel
BuckleySandler LLP

Emily Vaughn
Head of Accounts
Gem

Michael Zimits
President & COO
BCSI

Acknowledgements

The Chamber of Digital Commerce would like to acknowledge the following individuals from Deloitte for their contributions to the production of this white paper:

Deloitte Team

Mayank Singhal
Senior Consultant
Deloitte Consulting LLP

Prakash Santhana
Director
Deloitte Transactions & Business Analytics LLP

Abhishek Biswas
Senior Manager
Deloitte & Touche LLP

Soumak Chatterjee
Senior Manager
Deloitte Canada

Joan Cheney
Senior Manager
Deloitte & Touche LLP

Sachin Jade
Specialist Leader
Deloitte & Touche LLP

Sean Cremins
Business Technology Analyst
Deloitte Consulting LLP

Chashak Tulsyan
Business Technology Analyst
Deloitte Consulting LLP

Chamber Leadership

Perianne Boring
Founder and President
Chamber of Digital Commerce

Jason Brett
Director of Operations
Chamber of Digital Commerce

Dan Spuller
Director of Member Services
Chamber of Digital Commerce

Kevin Batteh
Chief Policy Advisor
Chamber of Digital Commerce

Ralph Benko
Senior Policy Advisor
Chamber of Digital Commerce

Chase Freeman
Blockchain Associate
Chamber of Digital Commerce

Overview

What Are Smart Contracts?

In 1996, Nick Szabo described a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[1] While the technology available to support smart contracts has evolved considerably since then, this definition continues to capture the essence of what a smart contract is and does.

Taking each element of Szabo's definition in turn:

"a set of promises"

- Depending on the model of smart contract deployed (see page 9: *What are the different models for smart contracts?*), such promises may be contractual or non-contractual
- They may consist of contractual terms and/or rules-based operations designed to carry out business logic

"specified in digital form"

- A smart contract operates electronically
- It consists of lines of code as well as the software that prescribes its conditions and outcomes
- Contractual clauses and/or functional outcomes are embedded as code within software

"protocols"

- A computer protocol in the form of an algorithm constitutes a set of rules for how each party should process data in relation to a smart contract
- Technology-enabled, rules-based operations enable actions to be performed, such as the release of payment

"within which the parties perform"

- The idea of automated performance is at the heart of a smart contract
- Driven in part by the technology that typically hosts a smart contract (that is, blockchain technology), smart contracts are traditionally regarded as irrevocable
- Once initiated, the outcomes for which a smart contract is encoded to perform cannot typically be stopped (unless an outcome depends on an unmet condition)

Smart Contract Models

What are the different models for smart contracts?

It is a common misconception that there is only one type of smart contract. In fact, there is a spectrum of possibilities.

Smart Contracts Lie on a Spectrum			
Contract entirely in code	Contract in code with separate natural language version	"Split" natural language contract with encoded performance	Natural language contract with encoded payment mechanism

Other permutations are, of course, possible and are likely to emerge as smart contract applications develop.

The role of code

The legal status of smart contracts is dealt with elsewhere in this white paper. For now, it is sufficient to note that smart contracts that seek to encode the entirety of a natural language contract (a "code is the contract" model) are very challenging from a legal perspective. The model puts into question an issue potentially relevant for all smart contracts: has a legally binding contract formed?

Smart Contract Models

Regardless of model the smart contract deployed, they all involve code. Code can contain bugs. Code may not always perform as the parties had intended. Messages transmitted over the internet can be delayed or interrupted, and data can be corrupted in transmission. Private encryption keys can be obtained by hacking. The liability implications of these kinds of events need to be carefully considered.

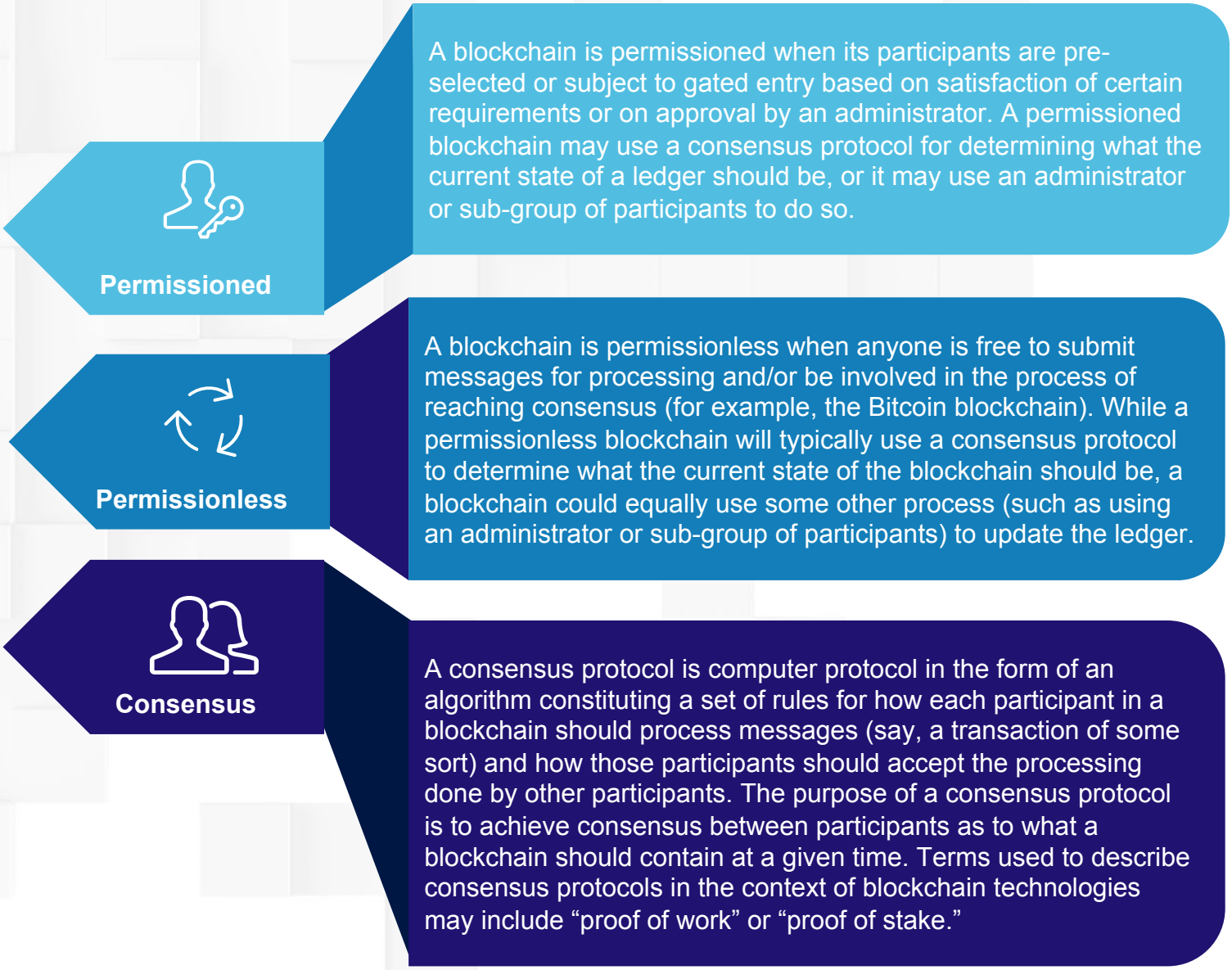
It is likely that once a model is demonstrated to work in a live environment, not only will it be adopted elsewhere, but smart contracts will, with developments in the underlying technology, incrementally become more sophisticated over time. It is quite possible that, within a relatively short timeframe, smart contracts will be doing significantly more than just automating aspects of the performance of a contract.

What makes up a smart contract?

Smart contracts are typically deployed on a blockchain (although it is possible for other platforms to host them too). Within a blockchain view of this, smart contract program logic sits within a “block.” A block is a software-generated container that bundles together the messages relating to a particular smart contract. Those messages may act as inputs or outputs of the smart contract programing logic and may themselves point to other computer code.

How Do Smart Contracts Work?

How is a typical smart contract initiated? It is necessary to have some understanding of the terminology:



How Do Smart Contracts Work?

the anatomy of a SMART CONTRACT

1 IDENTIFY AGREEMENT
- Multiple parties identify a cooperative opportunity and desired outcomes
- Agreements potentially in scope could include business processes, asset swaps, transferal of rights and more

2 SET CONDITIONS
- Smart contracts could be initiated by the parties themselves or by satisfaction of certain conditions like financial market indices, natural disasters or event via GPS location
- Temporal conditions could initiate smart contracts on holidays, birthdays and religious events

3 CODE THE BUSINESS LOGIC
- A computer program is written in a way that the arrangement will automatically perform when the conditional parameters are met

4 ENCRYPTION & BLOCKCHAIN TECHNOLOGY
- Encryption provides secure authentication and verification of messaging between the parties relating to the smart contract

5 EXECUTION & PROCESSING
- In a blockchain iteration, when consensus is reached on authentication and verification, the smart contract is written to a block
- The code is executed, and the outcomes are memorialized for compliance and verified

6 NETWORK UPDATES
- After performance of the smart contract, all computers in the network update their ledgers to reflect the new state
- Once the record is verified and posted to the blockchain, it cannot be altered, it is append only

Initiating a smart contract

Blockchain technologies use public key encryption infrastructure (PKI). Someone (we'll call this person the initiator) wishing to participate in a smart contract hosted on, say, a permissionless blockchain can:

- Download the software from publicly available sources
- Use an address (an alphanumeric character uniquely allocated to it by the software) to generate a public key
- Publish the public key on the system publicly

At the same time, the blockchain will also generate a corresponding private key for the initiator's address. This key is held securely by the software.

If the initiator wishes to trigger a smart contract transaction on the relevant ledger, it uses its address to send an initiating message, encrypted with its private key, to the other participants. The message is picked up by the participants' computers (called "nodes").

Messages purporting to be from the initiator's address can only be signed off on by a person in possession of the initiator's private key. Participants with access to the public key (which they receive from the software) can use it to verify that the smart contract transaction was initiated by the initiator in possession of the private key and to authenticate the message contents.

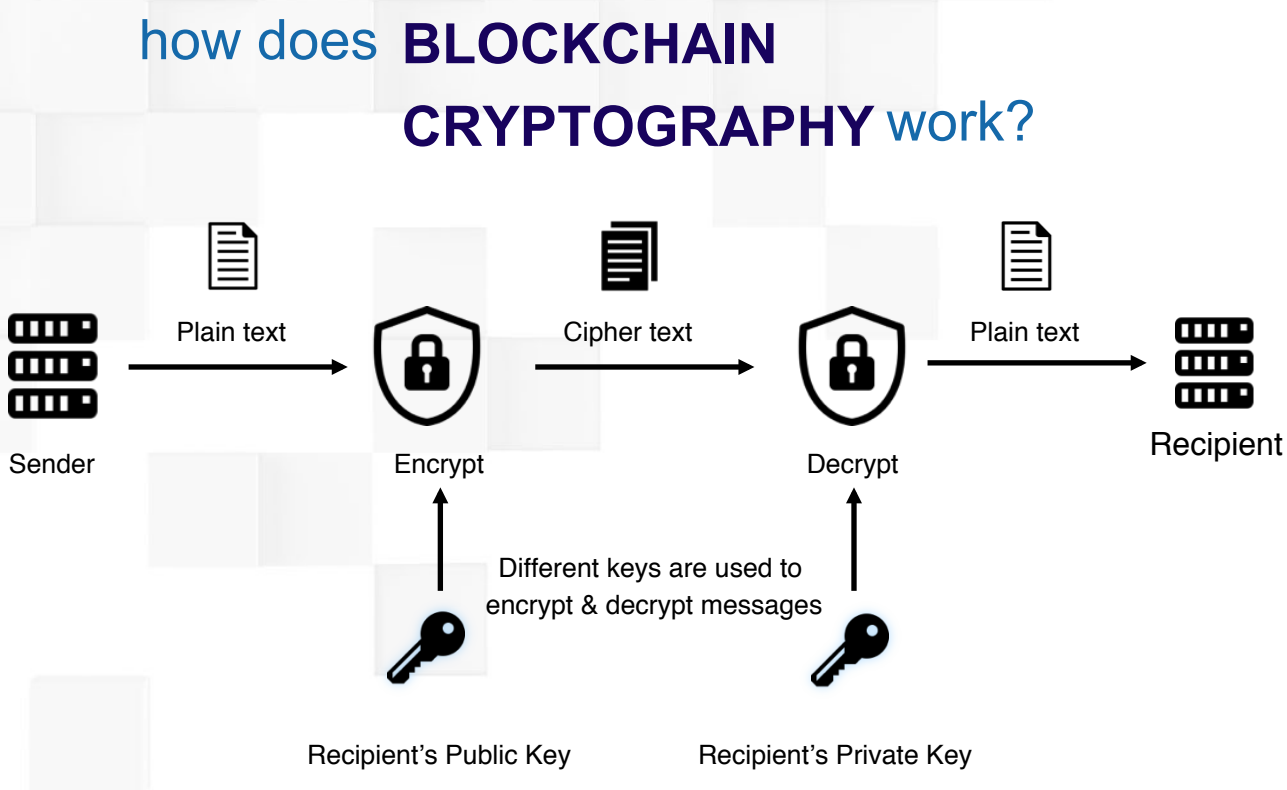
How Do Smart Contracts Work?

Writing a smart contract message to a blockchain

In a typical permissionless blockchain deployment, when a sufficient quantity of other participants or nodes, reach the same conclusion (more than 50 percent), the blockchain's applicable consensus protocol determines that the message relating to the smart contract should be added to the blockchain. Alternatively, such a determination might be reached by an administrator, in a permissioned blockchain.

Public key cryptography

As mentioned earlier, blockchain technology uses public key encryption infrastructure (PKI). PKI is a method of cryptography that uses of two types of keys. The first is a public key that all parties are aware of, and the second is a private key known only to its recipient. In a smart contract transaction initiated on a blockchain, the sending recipient encrypts their message into an unreadable 'cipher text' using algorithms or mathematical formulas, to protect and secure the data. Only the use of a private key can decrypt the 'cipher text' back into a readable 'plain text '. The key benefit PKI brings to smart contract transactions revolves around security, as it is extremely difficult, if not impossible, to reverse engineer a public key to a private one, making it very resilient to failures or hacks.



Use Cases

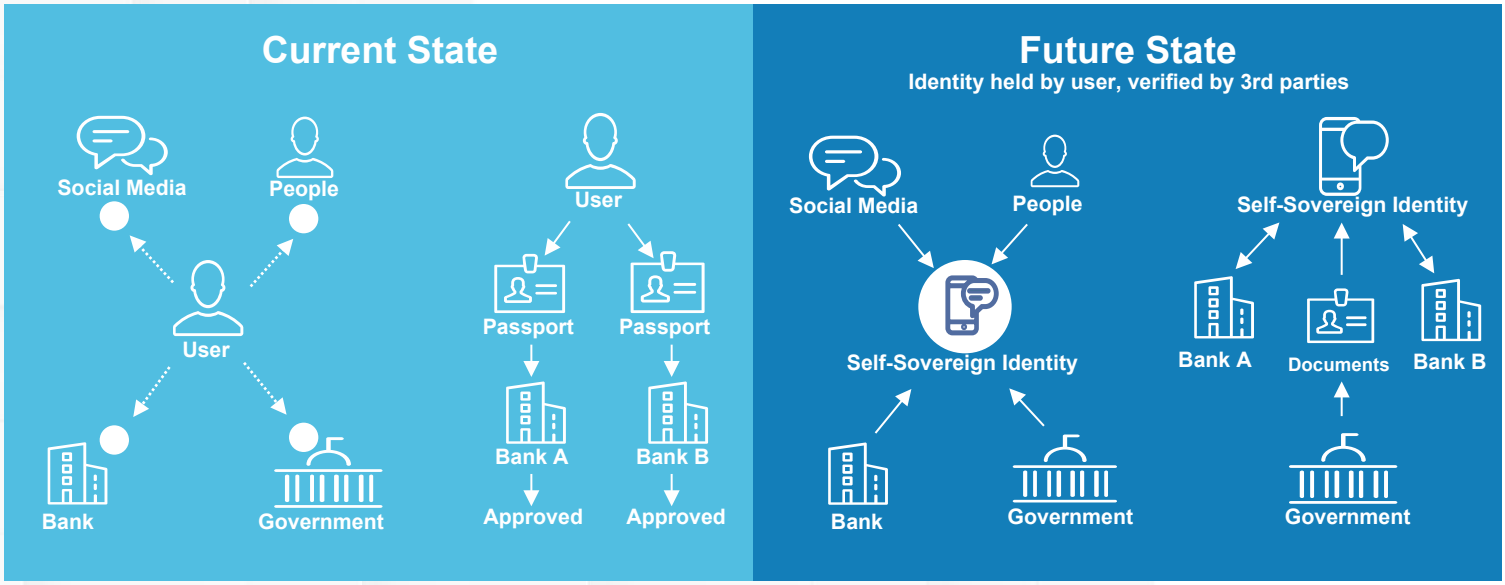
Twelve Use Cases for Smart Contracts

Smart Contracts for Digital Identity

Smart contracts can enable individuals to own and control their digital identity containing reputation, data and digital assets. This allows individuals to choose what personal data to disclose to counterparties, giving enterprises the opportunity to seamlessly know their customers.

Smart Contracts for Digital Identity

Self-sovereign digital identity enabled by smart contracts provides seamless, user-centered internet for individuals.



Current Challenges

- Expensive and time consuming Know Your Customer (KYC) processes that lack completeness
- Limited control over potential data leakage due to an individual's reliance on trusted third-parties
- High liability to safeguard user data presents a single point-of-failure and a target for hackers

Smart Contract Benefits

- Individuals own and control personal data (e.g. able to securely disclose personal data to various counterparties)
- Counterparties will not need to hold sensitive data to verify transactions, reducing liability while facilitating frictionless KYC
- Increased compliance, resiliency and interoperability

Smart Contract Considerations

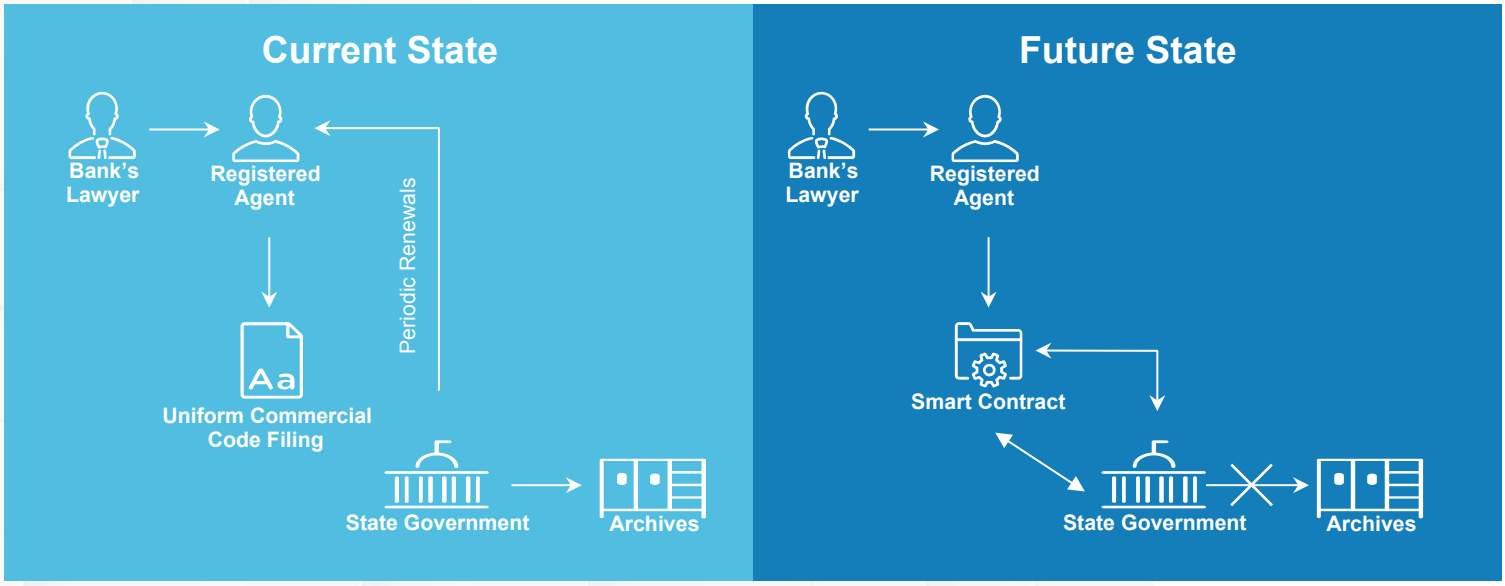
- Fostering an acceptance of digitally provided attestations within a legal framework and establishing trust in the security of smart contracts
- Technical integration with attestation providers
- Formation of protocols and standards to deliver interoperability by the involved parties

Smart Contracts for Records

Smart contracts can digitize Uniform Commercial Code (UCC) filing, and automate their renewal and release processes. Additionally, smart contracts can atomically perfect a lender's security interest at the moment of a loan creation.

Smart Contracts for Records

Automation of compliance, with rules requiring destruction of records on a future date enabled by smart contracts, and Uniform Commercial Code (UCC) liens that auto-renew, auto-release, or automatically call for collateral are all possible through smart contracts.



Current Challenges

- Paper-based filing for many foundational documents of finance with government
- Error-prone, manual process for renewing/ releasing Uniform Commercial Code filings results in latency
- Expired archival data stored with government occupies warehouses and incurs additional costs

Smart Contract Benefits

- Reduced legal bills through auto-renewal and auto-release of digitized UCC filings
- Automated processes, including calling by lenders for additional collateral and tracking of loan vs. collateral value
- Archival data automatically becomes unsearchable/unreplayable after it reaches its sunset date

Smart Contract Considerations

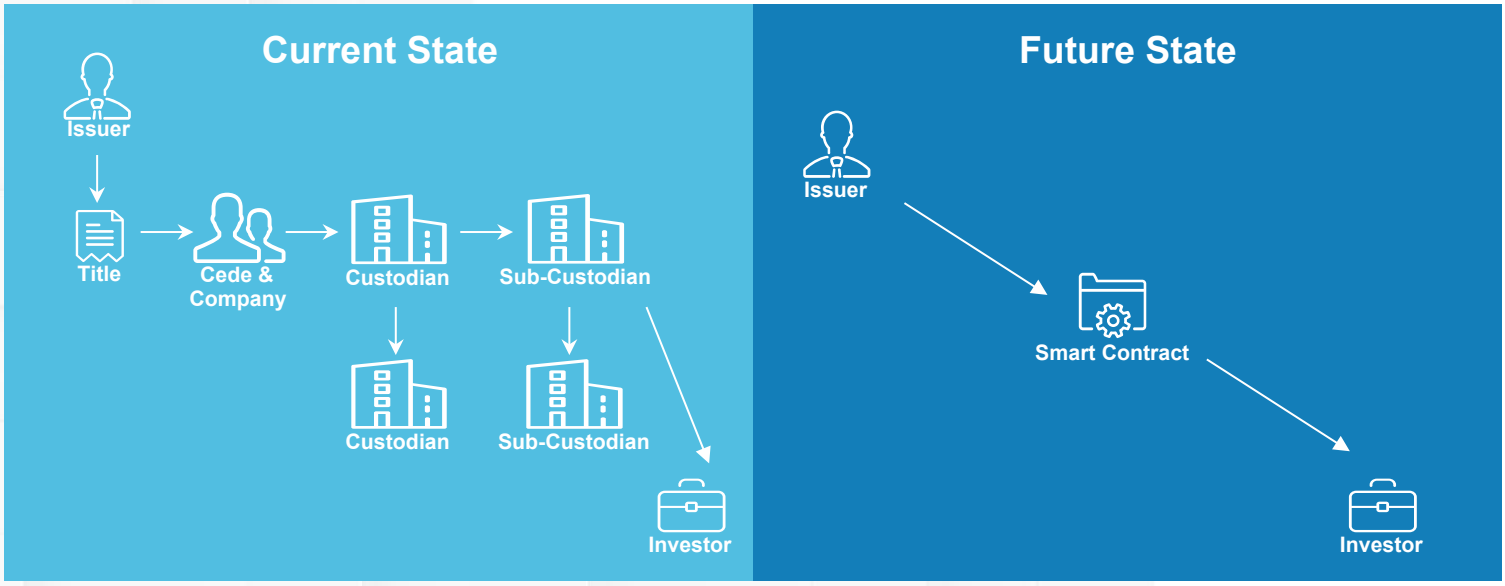
- Smart contract platform must be capable of storing data on a distributed ledger without slowing performance or compromising data privacy
- Active involvement of lenders and registered agents must exist for more complex functions (e.g. auto-release or automated call for additional collateral)
- Clarification regarding whether courts would consider a document legally destroyed if it is merely cryptographically unsearchable rather than removed from the ledger

Smart Contracts for Securities

Capitalization table management can be simplified, and intermediaries circumvented in the chain of securities custody through the implementation of a smart contract. The smart contract can facilitate the automatic payment of dividends, stock splits and liability management, while reducing counterparty and operational risks.

Smart Contracts for Securities

Simplification of capitalization table management for private companies can be enabled by smart contracts, while also reuniting record ownership with beneficial ownership of publicly traded securities, reducing cost, and counterparty risk.



Current Challenges

- Paper-based, manual corporate registration processes
- Companies that fail to keep their corporate registrations up-to-date require clean-up and certificate of good standing before issuing securities
- Intermediaries increase cost, counterparty risk and latency

Smart Contract Benefits

- Digitized end-to-end workflows due to securities existing on a distributed ledger
- Trade date plus zero days (T+0) securities settlement cycles
- Facilitates automatic payment of dividends and stock splits, while enabling more accurate proxy voting
- Removes counterparty and operational risks created by intermediaries

Smart Contract Considerations

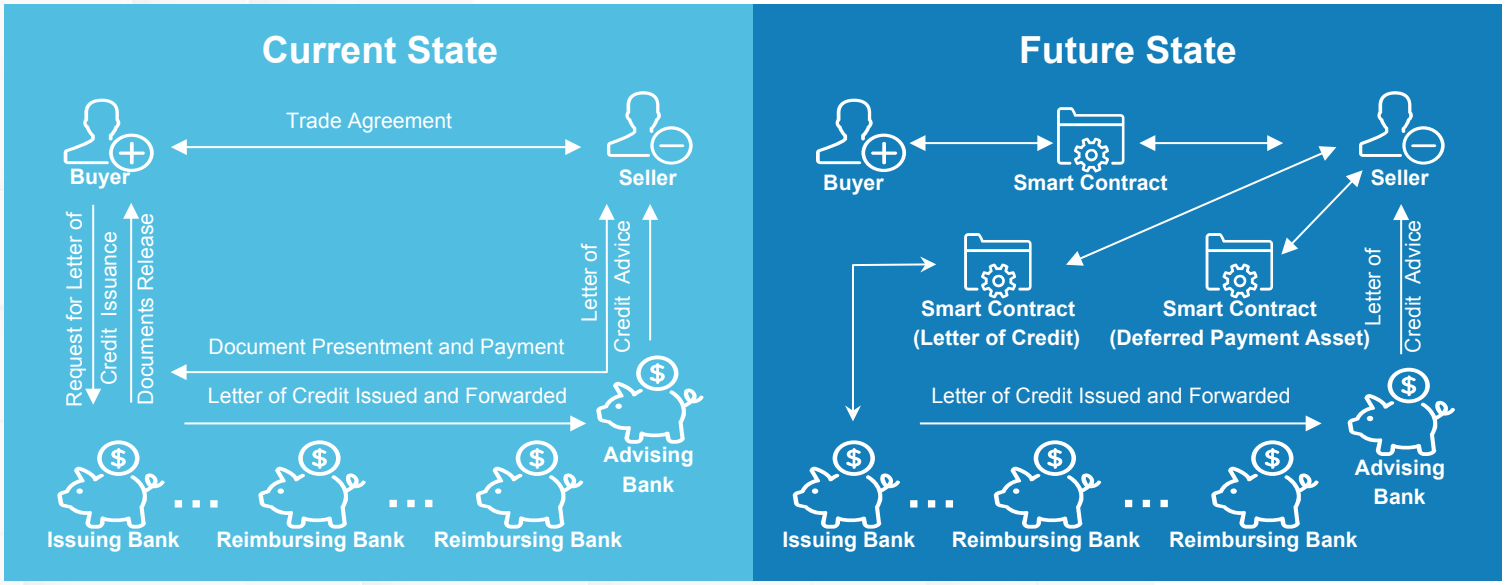
- Benefits may be realized more quickly in private securities markets than in public securities markets
- The cryptographic signature of the State of Delaware on the ledger entry takes the place of the State's seal on paper stock certificates, which may require enabling legislation to clarify that Delaware corporate law permits registration on a distributed ledger
- While issuers would welcome visibility into who owns their securities, some buy-side firms (e.g. activist investors) carefully protect this information

Smart Contracts for Trade Finance

Smart contracts can facilitate streamlined international transfers of goods through faster Letter of Credit and trade payment initiation, while enabling higher liquidity of financial assets.

Smart Contracts for Trade Finance

Payment method and instrument automation enabled by smart contracts provides risk mitigation and improved financing and process efficiencies for buyers, suppliers and financial institutions.



Current Challenges

- Time-consuming and costly Letter of Credit issuance process due to required coordination and paperwork
- Physical document management can delay shipment receipt until title document is released
- High document fraud/duplicate financing due to de-linked processes

Smart Contract Benefits

- Faster approval and payment initiation through automated compliance and monitoring of Letter of Credit conditions
- Improved efficiency in creating, modifying and validating trade, title and transport-related contract agreements
- Increased liquidity of financial assets due to ease of transfer and fraud reduction

Smart Contract Considerations

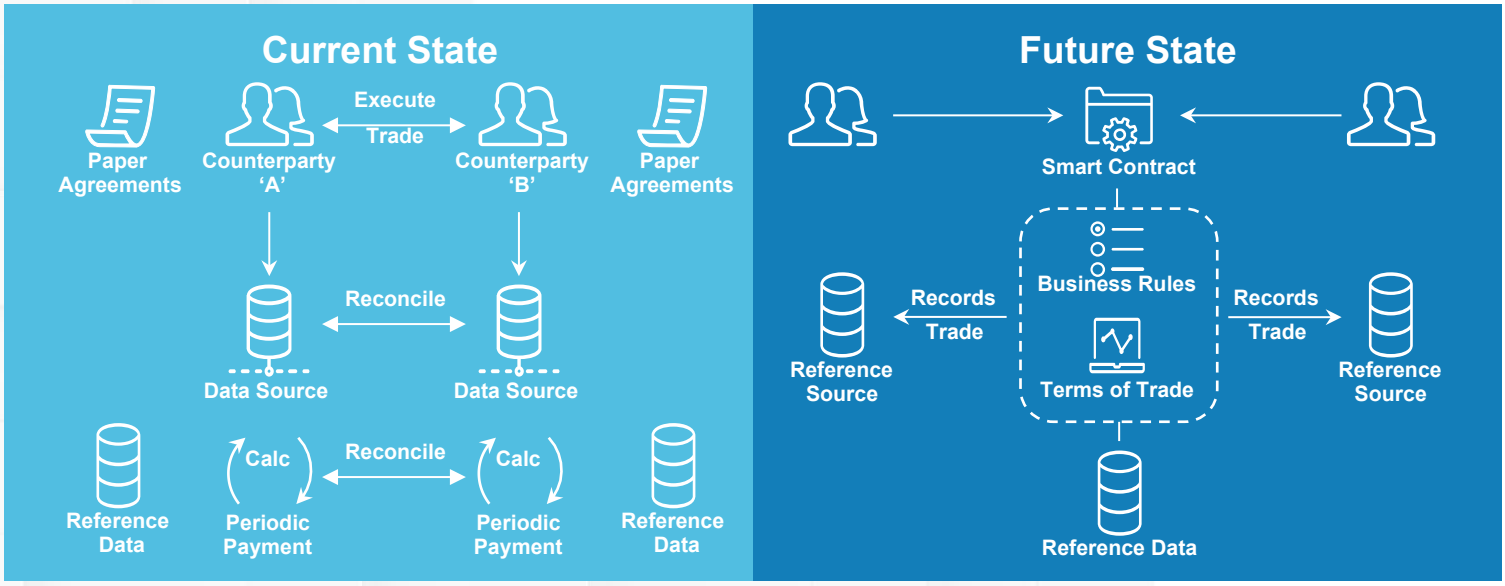
- Industry-wide standards for smart contract templates and procedures must be implemented for wider acceptability and adoption
- Legal implications for potential smart contract execution fall-out must be determined (in particular for defaults and dispute resolution)
- Integration with settlement systems, off-chain ecosystems and technology prerequisites (e.g. Internet of Things) must be successful to achieve full benefits

Smart Contracts for Derivatives

Post-trade processes can be streamlined through smart contracts, eliminating the duplicative processes performed by each counterparty for recording and verifying trades, and executing applicable trade level and other lifecycle events

Smart Contracts for Derivatives

Enforcing a standard set of rules and conditions to a transaction enabled by smart contracts optimizes post-trade processing of over-the-counter (OTC) derivatives.



Current Challenges

- Redundant and time-consuming processes due to asset servicing being managed independently by each counterparty for most OTC derivatives
- Paper-based transaction agreements that contain terms, trade agreements and/or post-trade confirmations

Smart Contract Benefits

- Automated settlement of obligations while executing triggered processing of trade events (e.g. periodic payments)
- Automated external event processing (e.g. credit) and/or succession events
- Enabled real-time valuation of positions for real-time exposure monitoring, while reducing errors and/or disputes

Smart Contract Considerations

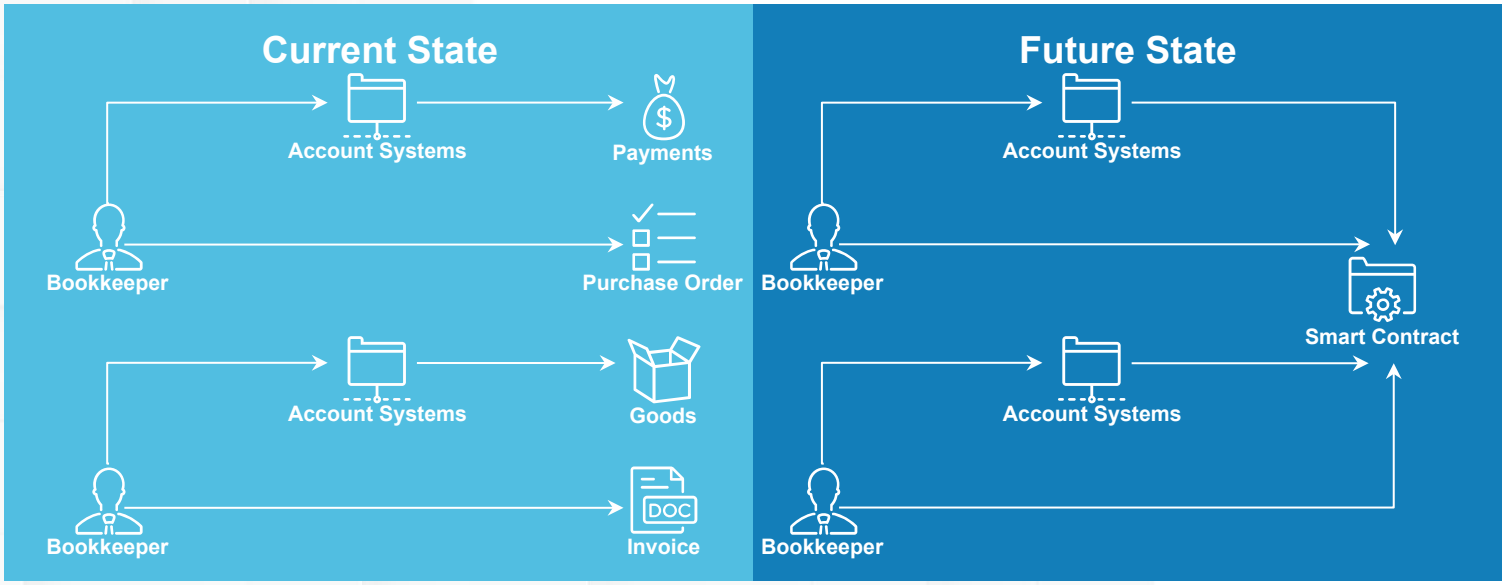
- Establish proper governance of a blockchain network and its smart contracts to properly manage large-scale protocol changes to existing contracts due to regulatory reform, change in contract or other unforeseen events
- Agreement upon lifecycle events for OTC derivatives (e.g. external source of data)
- Integration and governance of oracles required to feed smart contracts with information to/from the blockchain network

Smart Contracts for Financial Data Recording

Financial organizations can leverage smart contracts for accurate, transparent recording of financial data. Smart contracts enable uniform financial data across organizations, improved financial reporting and reduced auditing and assurance costs.

Smart Contracts for Financial Data Recording

Smart contracts enable accurate recording of financial data for entities entering into financial transactions.



Current Challenges

- Accounting systems are prone to fraud and errors since they are controlled directly by entities
- Capital intensive processes due to each firm maintaining their own infrastructure
- Significant human capital/middleware required to process transactions from systems that do not interoperate

Smart Contract Benefits

- Improved transactional data integrity and transparency, yielding increased market stability
- Reduced expenditure for accounting information systems by cost-sharing across multiple organizations
- Improved insight into parties' capital due to increased financial accessibility

Smart Contract Considerations

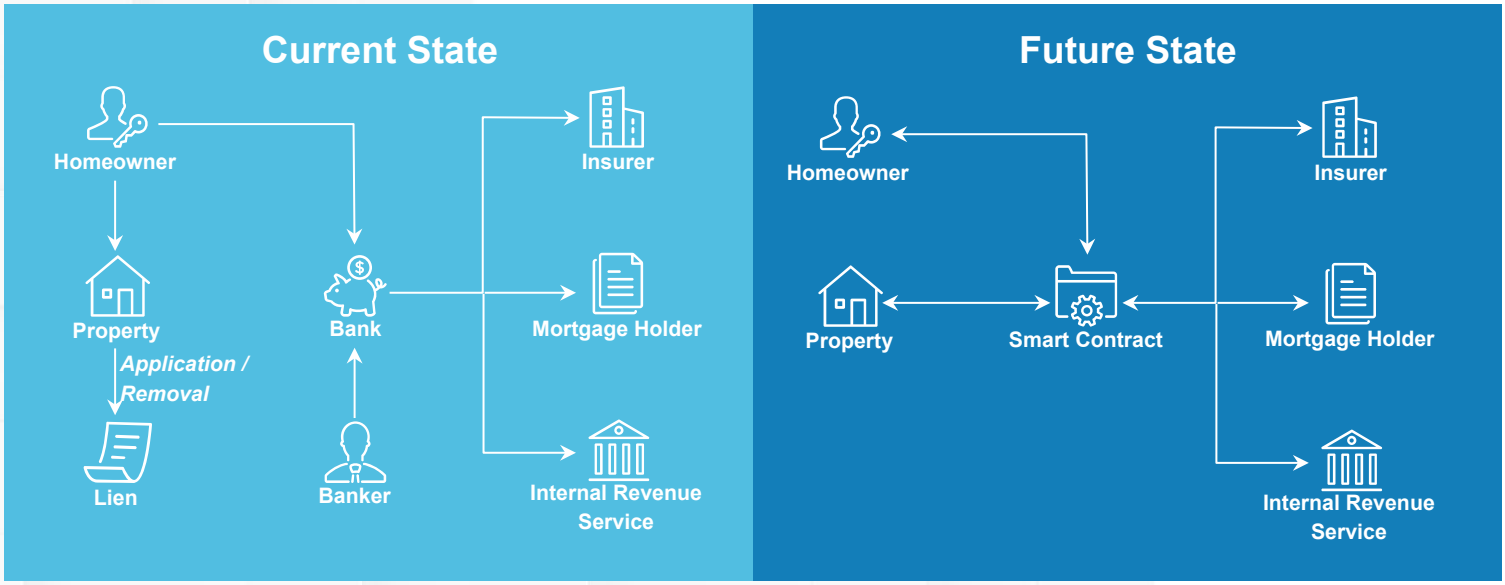
- Development of a portal to streamline smart contracts that facilitate and report financial transactions
- Design a set of standards for tokenized assets
- Interoperability between a distributed ledger network and legacy systems
- Creation of a marketplace of attesters to audit financial smart contracts

Smart Contracts for Mortgages

Smart contracts can automate the otherwise confusing and manual process behind a mortgage contract. A smart contract in this case automatically connects the different parties involved with mortgage transactions, allowing for a frictionless and less error-prone process.

Smart Contracts for Mortgages

Mortgages enabled by smart contracts provide automated processing of payments and release of liens on property.



Current Challenges

- Process friction includes: payment application, updating balances, disbursing payments and taxes, and releasing liens when a mortgage is paid off
- Interface with auxiliary and dependent processes (e.g. land records)
- Privacy concerns due to security holders' needing to know borrowers' identities

Smart Contract Benefits

- Automated release of liens from land records when mortgage is paid off
- Increased visibility of servicer records to all interested parties, enabling payment verification and tracking
- Reduced cost and errors by elimination of manual processes

Smart Contract Considerations

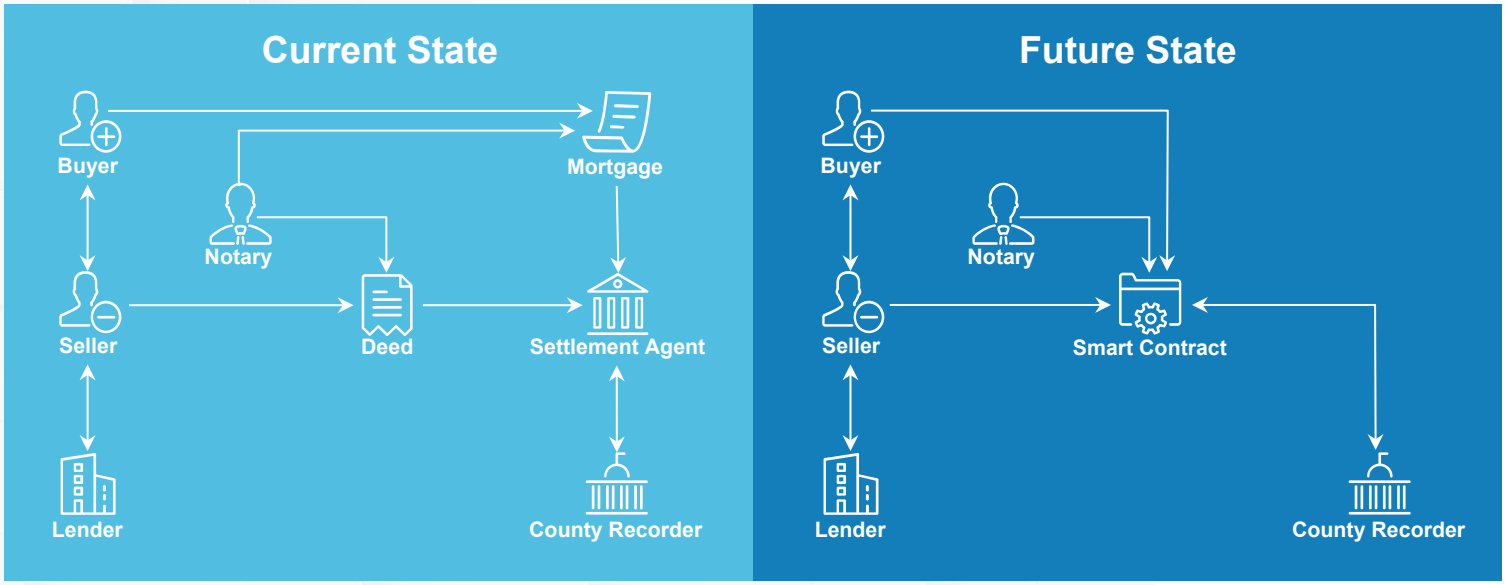
- Development of an interface between contract, borrower payment account, disbursement accounts and real estate title record service
- Digital identity must be successfully implemented to enable this use case
- Adoption of public key infrastructure between a mortgagee and the many parties involved

Smart Contracts for Land Title Recording

By facilitating property transfers through smart contracts, fraud propensity can be reduced while increasing confidence in identity. These transactions can occur with increased efficiency and transparency, and costs for auditing and assurance can be reduced.

Smart Contracts for Land Title Recording

Property transfers enabled by smart contracts can deter fraud and improve transaction integrity, efficiency and transparency.



Current Challenges

- Capital intensity due to incompatible infrastructure
- Unreliable identity verification and signing process for notarized documents
- Manual processes delay steps and create potential for document alteration
- Multiple parties can be shown the same property without detection

Smart Contract Benefits

- Changes in insurance and risk due to delivery assurance (from visibility)
- Higher confidence in identity of parties, streamlined processes and reduction in auditing/assurance costs
- Automated process notifications and incorporation of integrity protections
- Eliminate shotgunning mortgage fraud

Smart Contract Considerations

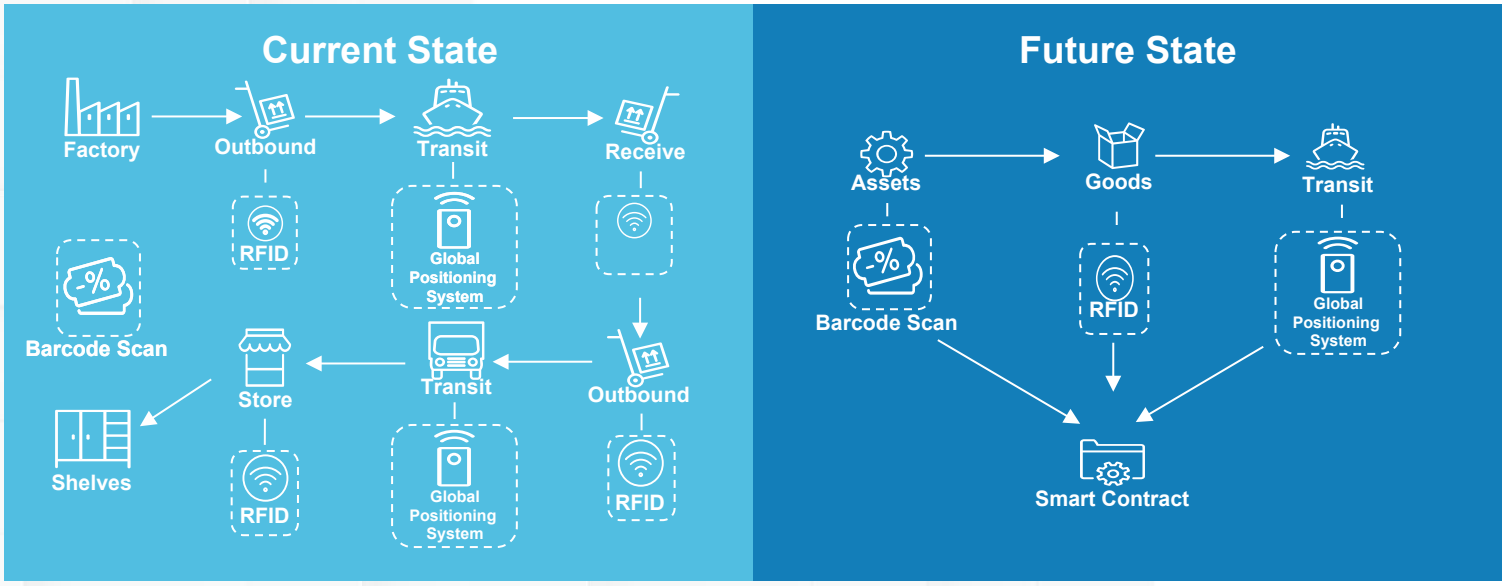
- Standardized record format (such as data elements and signature fields) must be used by participating entities for deeds
- Common protocols must be developed for communication with recording offices and electronic recording file formats
- Federated identity credentials must be accepted

Smart Contracts for Supply Chain

Smart contracts can provide visibility at every step of a supply chain. Internet of Things devices can write to a smart contract as a product moves from the factory floor to the store shelves, providing real-time visibility of an enterprise's entire supply chain.

Smart Contracts for Supply Chain

Extended supply chain visibility, enabled by smart contracts, provides stand-up and tear-down of goods tracking across brands, retailers, logistics and contracted counterparties.



Current Challenges

- Limited visibility due to siloed data capture and desire to only share information with relevant parties
- Need for captured data to be similarly formatted to extract values
- Incompatibilities in data and blind spots in tracking goods due to silos in the supply chain (even source-tagged goods)

Smart Contract Benefits

- Simplification of complex multi-party systems delivery
- Achieve granular-level inventory tracking and delivery assurance, potentially improving supply chain financing, insurance and risk
- Enhanced tracing and verification to reduce risk of fraud and theft

Smart Contract Considerations

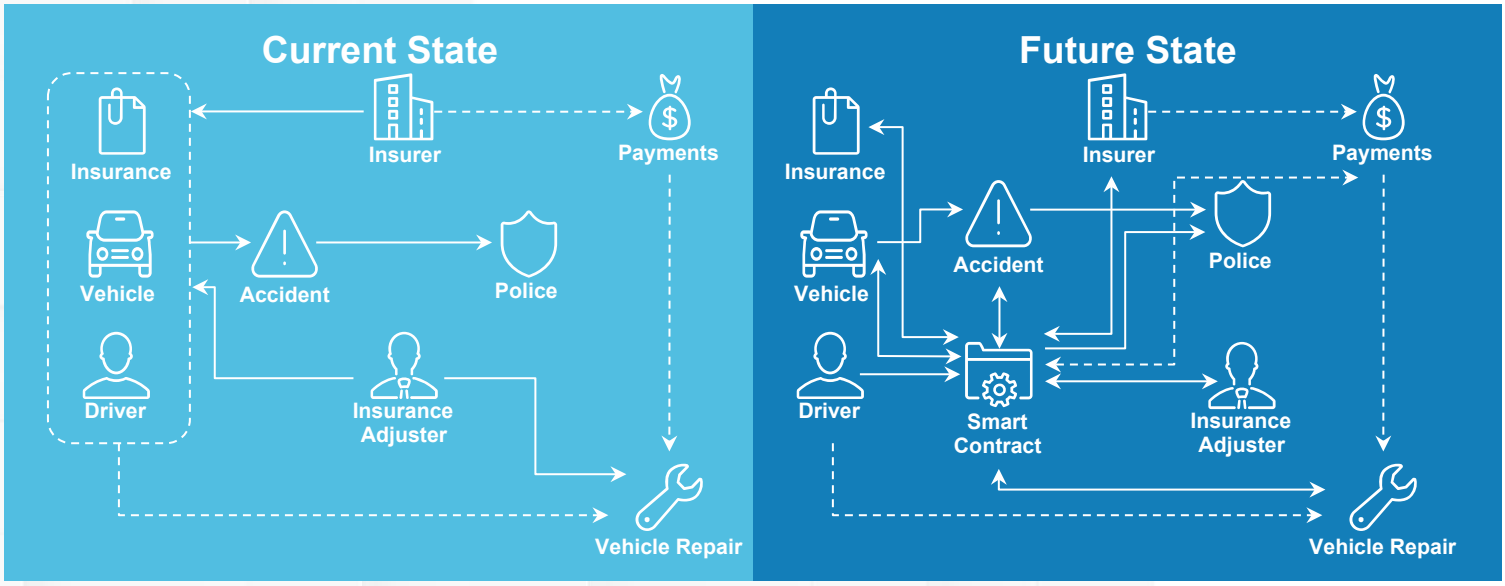
- Trusted oracles must be implemented to provide validated registrations of an entity
- Identities must be registered and attested over time, including for institutions, individuals, sensors, facilities and goods

Smart Contracts for Auto Insurance

Currently, the car insurance claims process is disjointed, but the process can be improved significantly through smart contracts. The smart contract records the policy, driving record and reports of all drivers, enabling Internet of Things-equipped vehicles to execute initial claims shortly after an accident.

Smart Contracts for Auto Insurance

Automated insurance claims enabled by smart contracts provide instantaneous processing, verification and payment by vehicles that are able to communicate with each other and assess and validate their own condition.



Current Challenges

- Multiple forms, reports and data sources yield increased error propensity and wasted time/resources
- Duplicated work due to insurance provider devoting back-office resources to verify records, reports and policies
- Subjective diagnostics during processes increases costs and delays

Smart Contract Benefits

- Repository for each policy holder includes global driving record, policy, vehicle type and accident report history
- Vehicle “self-awareness” and damage assessment using sensors can execute initial insurance claims/police reports
- Increased savings by reducing duplicated work to verify reports and policies

Smart Contract Considerations

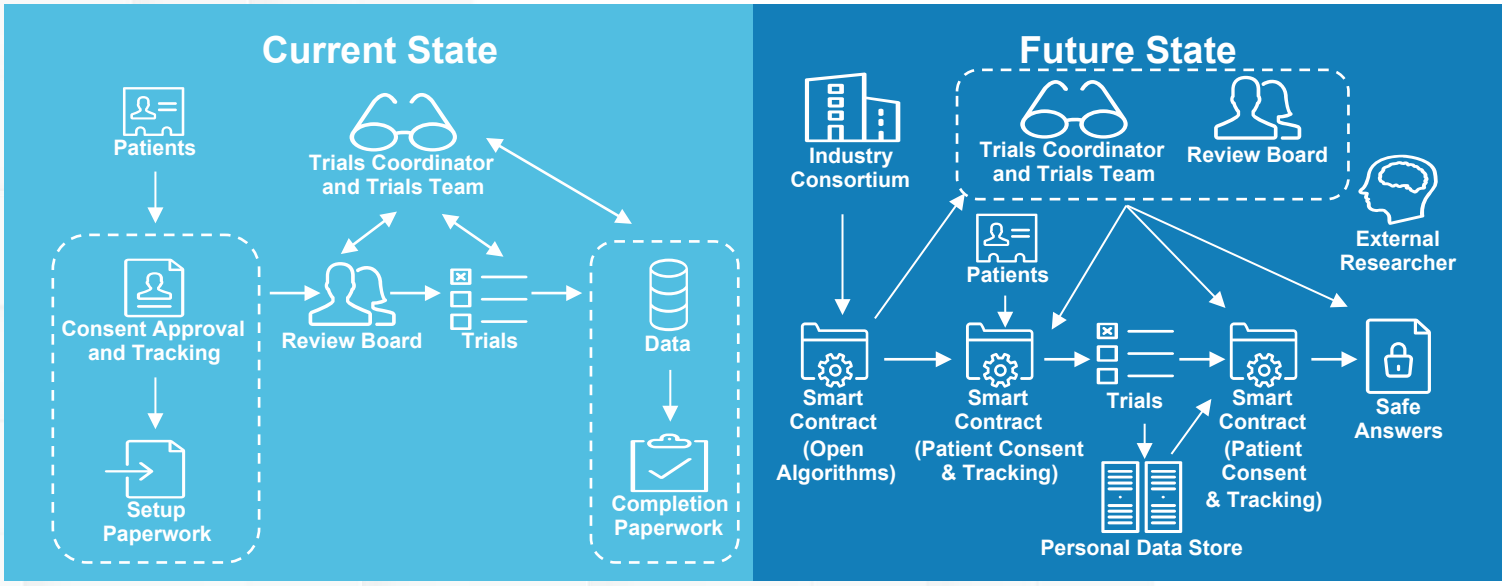
- Distributed Autonomous Policy (DAP) for ride-sharing companies that use contractors’ cars and labor could be implemented, representing bundled, scalable and self-executing policies based on a driver’s record, vehicle type and performance
- Innovation, cross-industry collaboration, and an environment open to testing and failing must be achieved to navigate the technological, financial and regulatory challenges

Smart Contracts for Clinical Trials

Clinical trials can benefit from smart contracts through increased cross-institutional visibility. The smart contract includes privacy-preserving computation that improves data sharing between institutions while automating and tracking consent for patient data.

Smart Contracts for Clinical Trials

Increased visibility enabled by smart contracts may streamline the clinical trials process by increasing the sharing of data for participants in the ecosystem.



Current Challenges

- Delays in responding to epidemics due to friction in sharing data from clinical trials
- Limited understanding of treatment harms/ benefits due to under-reporting
- Limited patient involvement due to lack of consistent consent management
- Comprisable patient privacy and re-identification due to sharing datasets

Smart Contract Benefits

- Increased visibility and reduced costs by streamlining setup processes for trials
- Improved access to cross-institution data during epidemics, protected by privacy-preserving computation
- Increased automation in obtaining and tracking consent for shared data access
- Increased confidence in patient privacy

Smart Contract Considerations

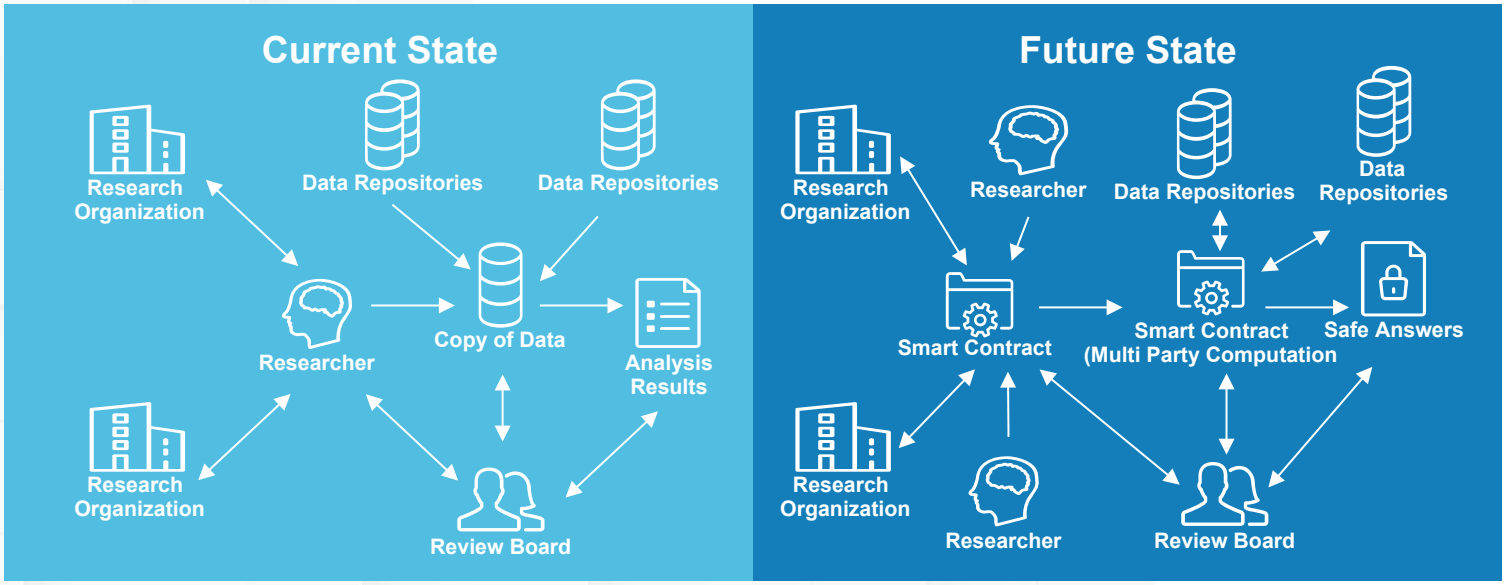
- Potential to cause positive disruption in the clinical trials community by providing scale to privacy-preserving data-sharing techniques and new multi-party computation architectures
- Identity, authentication and authorization remain open issues for smart contracts executable on blockchain enabled networks
- Potential path forward for the evolution of new data markets (e.g. clinical trials data market) based on new economic incentives models

Smart Contracts for Cancer Research

Smart contracts can facilitate the sharing of cancer data throughout a cancer research consortium. The smart contract can facilitate the otherwise cumbersome patient consent management process and incentivize aggregate data contribution and data sharing while maintaining patient privacy.

Smart Contracts for Cancer Research

Unleashed power of data enabled by smart contracts provides more efficient data sharing across sectors and incentivizes pre-competitive collaborations.



Current Challenges

- Cumbersome processes for sharing research across institutions
- Discouraged sharing of research due to privacy concerns
- Hindered data collection due to lack of trust and real-time access to patient data
- Deterred data sharing due to concerns around misaligned incentives

Smart Contract Benefits

- Enhanced data sharing while observing patient privacy/regulatory requirements
- Real-time visibility and policy enforcement incentivizes sharing without divulging raw data
- Increased volume of data and trust due to smart contract patient consent management

Smart Contract Considerations

- Standardization of privacy-safe queries and their representation in smart contracts must occur before benefits can be realized
- Transparency into allowable queries and available datasets backed by “open algorithms” that are vetted by experts must exist to ensure confidentiality
- Real-time access and protection of data confidentiality may require development of new forms of blockchain technologies

Legal and Regulatory

Introduction

As stated in the beginning of this paper, there is 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. While smart contract code adds new facets to legal analysis, it is much more straightforward to see how contract law will apply when parties simply use code to implement natural language contracts because the natural language contract is still the entire agreement. When the code becomes the contract, resulting in a separate and distinct form of smart contract, there are many other issues raised, and the application of contract law becomes more complicated.

It is not anticipated that smart contracts will displace the long-standing pillars of contract law (including offer, acceptance and consideration) in either situation. However, for smart contracts written entirely in code, courts will face additional challenges in applying contract law to determine when or whether a contract has formed, whether a party has performed its obligations, whether a party has breached and other related issues. Contract law developments in the context of online agreements and other agreements aided by technology provide significant guidance for how contract law will apply to smart contracts in both situations.

An example of a recent technological change is the internet and the rise of natural language contracts in computerized (or electronic) form. Over the past decade, regulators and courts have come to accept electronic contracts in the financial services area. For instance, the federal electronic signature law[2] (ESIGN), enacted in 2000, and subsequent state implementation of the Uniform Electronic Transaction Act[3] (UETA) have led to widespread use of electronic contracts and electronic records. Courts have enforced natural language electronic contracts. Consumers can now purchase car insurance online and deposit checks via their smartphones. Regulators have become comfortable with many regulated transactions moving to purely electronic form.[4]

With respect to Fintech, regulators approach and view innovation differently but, in general, cautiously support the new technology. The Office of the Comptroller of the Currency[5] and the Consumer Financial Protection Bureau[6] have indicated support for innovation, while the Federal Reserve has indicated that the technology requires “much more complex demonstrations in real-world situations before these technologies can be safely deployed in today’s highly interconnected, synchronized and far-reaching financial markets.”[7]

Regulators will likely be more interested in regulating the functions and impact of any new technology rather than the technology itself, as was the case with transactions moving to purely electronic form. New technologies can raise unique issues that may draw regulatory scrutiny or new requirements (e.g., encryption). This section explores some of the many legal and regulatory issues that smart contracts raise, including creating and performing a smart contract, handling disputes, complying with regulatory requirements and providing access to regulators.

Creation of the Smart Contract

Businesses commonly use clickwrap agreements—also referred to as “click-through” or “click and accept” agreements—to present terms and conditions of use to consumers who may in turn agree with the click of an “I Accept” button. Despite their initial novelty, courts now generally recognize clickwrap agreements as helpful and enforceable forms of contracting.[8] In certain situations, when determining what to enforce, courts have closely examined whether the consumer received notice of the existence of a term before agreeing to it.[9] For example, courts have been apprehensive in certain instances to bind parties in situations where additional terms to an agreement were emailed after acceptance.[10] Additionally, the use of a website without explicit notice of the conditions of use (which were merely posted on the homepage) has also been deemed insufficient acceptance of those terms, especially in the consumer context.[11]

Whether a contracting party has been given requisite notice of a term depends on how conspicuous the term is, the sophistication of the parties involved and their past dealings, and industry practice.[12] As with clickwrap agreements, courts will need to develop standards to determine when a smart contract or term therein will be enforced, and they will likely employ notice as a key determinant. In the case of smart contracts where the “code is the contract,” parties may experience more difficulty proving that they provided notice of terms contained in the code, especially with less sophisticated customers.

Also, in “code is the contract” situations or situations where a portion of the contract is contained in code, parties may have to confront issues related to the Statute of Frauds. The Statute of Frauds, where and when it applies, requires certain agreements to be made in writing and parties may challenge whether code is sufficient to serve as a writing. It will be important to provide parties with confidence that code can survive a Statute of Frauds challenge.

A related consideration is the extent to which electronic agents can make decisions through smart contract code that bind their principals. Limited precedent already exists in the United States. At one end of the spectrum, the automatic issuance of a tracking number has been deemed “an automated, ministerial act” that does not constitute contractual acceptance.[13] At the other, a court has held an insurance company liable for its computerized reinstatement of an insurance policy, citing the following: “A computer operates only in accordance with the information and directions supplied by its human programmers. If the computer does not think like a man, it is man’s fault.”[14]

Furthermore, in equities markets, a customer can place limit orders “where the customer specifically instructs the market maker to execute a trade when the stock reaches a particular price.”[15] In essence, the customer provides an advance instruction to a broker to execute a trade on the customer’s behalf when a specified price is reached. U.S. courts have discussed limit orders in detail without questioning that the customers are bound by the resulting transactions.[16] Accordingly, courts and lawmakers will likely look for the level of control principals have over their electronic agents and the principal’s act of instructing an electronic agent to perform tasks on its behalf.

Creation of the Smart Contract

Regulators may also look to the formation of smart contracts as an opportunity to provide consumer protection. Regulators could require parties to hard-code certain terms or regulatory conditions into smart contracts as an enforcement tool. As an example, regulators could require parties to loans to input maximum interest rates to prevent usury and monitor for compliance. Coding requirements could lead to conflicts-of-law problems for companies who must answer to multiple federal regulators and the rules of several states (such as usury), especially when regulations change.

Considerations for Smart Contract Creation

- Notice of Terms to Parties
  - Visibility (are terms conspicuous?)
  - Timing (were terms shared before or after agreement?)
  - Difficulty (how hard must consumer work to see terms?)
- Sophistication of Parties
- Level of Control over Electronic Agents

Performance of the Smart Contracts

As this paper has shown, smart contracts hold promise for automated performance in a variety of business use cases. A few examples where contract performance should be straightforward include:

- **Insurance Contracts** in which the parameters of an insurance policy are written into smart contract code and enforced automatically. The policy would, for example, pay out insurance proceeds upon the occurrence of an independently determined insurable event (e.g. wind speed over 70 miles per hour for 10 consecutive minutes) without the need to make a claim;[17]
- **Escrow** in which a smart contract protocol sequesters messages or funds held on a distributed ledger until the occurrence of some event and the verification of message content. Once the event occurs and the content has been verified, the smart contract protocol automatically performs a stated contractual action (e.g., the payout of a certain amount of escrowed funds or the delivery of bearer certificates);[18]
- **Royalty Distribution** involving the automatic payment of artists and other associated individuals pursuant to the terms of a contract.[19]

Other contracts may involve much more difficult, oftentimes subjective, judgment which will make automated performance more difficult. For example, smart contracts may be difficult to develop and implement where the situation calls for: (1) reversibility of transactions; (2) subjective analysis (how much flood damage was there on the second floor of a building?); (3) the programming of excessively complex or nebulous principles into smart contract code (e.g., interpretational standards, such as "reasonableness"); or (4) extensive interaction between a blockchain and the outside world (i.e., data input from outside the ledger or an impact on the outside world by events on a ledger).

Parties must determine other issues even when smart contracts call for objective "outside data." An example of the "outside data" aspect of a blockchain would be in the context of flood insurance: who decides when the rainfall threshold is reached? Parties will have to agree in advance to make the determination. For example, the parties may agree to use rainfall data compiled by the National Weather Service. Parties will also need to agree to sufficient "fallback" providers if the primary source is no longer available and the extent to which they can challenge the outside data.

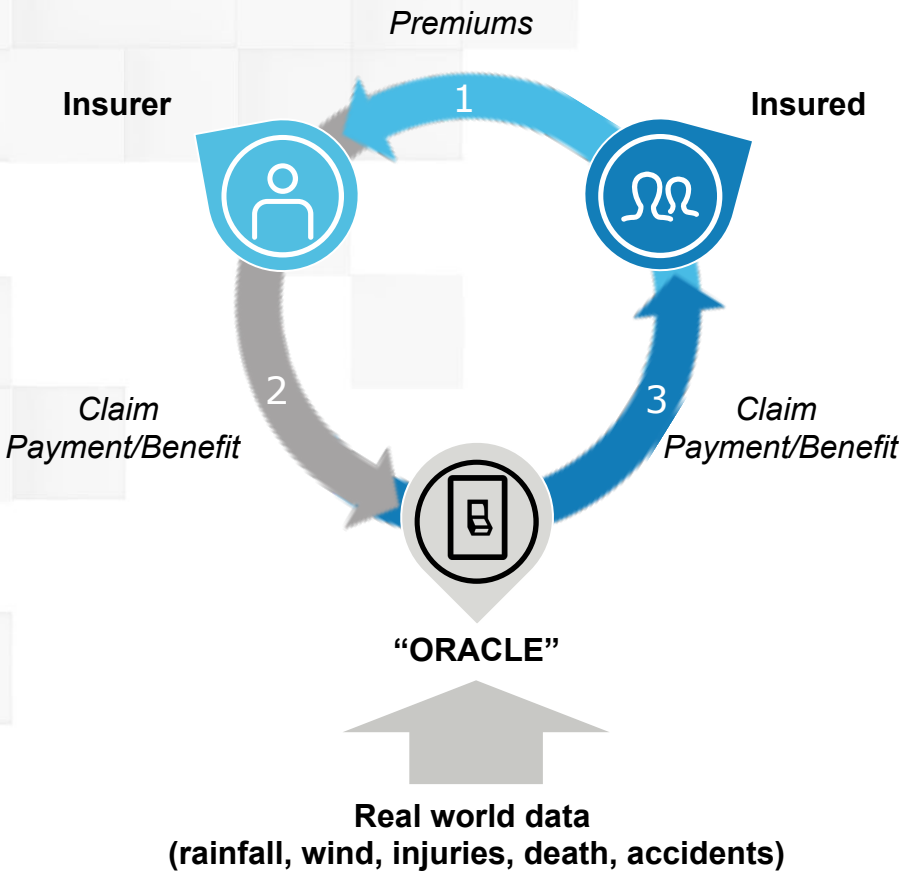
Performance of the Smart Contract

The parties will also need to agree on how the information will make its way to a blockchain. Algorithmic platforms, known as “oracles,” whose sole task is to feed information from the outside world into the ledger to facilitate smart contract enforcement, will perform the data-input function.[20] The outside actor must be a trusted third party and must preserve the integrity of the smart contract by transmitting accurate and trustworthy data in a secure manner.

In the reverse situation, the parties to a ledger-hosted smart contract may intend for an event on the hosting ledger to affect the outside world. Without involvement from a trusted third party, however, enforcement is limited to the particular blockchain. Complex smart contract proposals may call for off-ledger assets to be moved, such as physical goods or funds held in a bank, upon the occurrence of some event on a blockchain. In such a situation, the parties would enlist a trusted third party (potentially a financial institution) to monitor the blockchain and respond to events as required.

Automated Performance Example

1) Insured pays premiums to insurer
2) Insurer makes funds available to pay claims and benefits
3) Payments and benefits are automatically disbursed when the ”oracle” determines the occurrence of specified events



Dispute Resolution and the Role of Lawyers

Some believe that smart contracts will help rid the world of lawyers[21] and render final decisions on who wins and loses free from the influence of lawyers. Nevertheless, while smart contracts are intended to mimic complex decision-making, someone—possibly a lawyer—will create the code that renders the often intricate legal decisions needed to construct a workable commercial contract. Organizations will likely still employ traditional lawyers to negotiate actual terms and perform due diligence.[22] In fact, smart contracts may require new types of due diligence by lawyers to provide comfort that the code is enforceable and embodies the intended provisions. Still, in light of "computer protocols that facilitate, verify, execute and enforce the terms of a commercial agreement,"[23] ledger-hosted smart contracts can streamline financial transactions and potentially reduce legal expense.

In the context of disputes, a number of competing concepts will determine the level of involvement of lawyers and courts. For instance, despite the attractiveness of the certainty afforded by a smart contract, contract law needs a level of flexibility to handle subjective issues. It will be more challenging for coders to build good faith, fair dealing and other subjective concepts into smart contracts, and there may be more of a role for judges, juries and arbitrators to decide matters when they involve subjective issues.

To determine the proper forum for resolving smart contract disputes and the rights of parties to access the courts, if any, we can look to the law of waiver and arbitration for guidance. In general, "parties to a contract may voluntarily waive certain rights, including the right to receive an impartial and independent federal adjudication, otherwise available to the parties under the law."[24] United States courts have enforced arbitration agreements that preclude judicial review of an arbitration award beyond the trial court level.[25] Similar waivers have been upheld in international forums.[26] In *AT&T Mobility LLC v. Concepcion*,[27] the U.S. Supreme Court held that the Federal Arbitration Act (FAA) preempted a California judicial rule stating that a class arbitration waiver was unconscionable under California law.[28] Consequently, there is significant precedent for expediting resolution and restricting access to courts.

Dispute Resolution and the Role of Lawyers

Recently, however, the United States has seen a resurgence of resistance to mandatory arbitration, particularly in the retail consumer context. As an example, the Consumer Financial Protection Bureau (CFPB) recently proposed rules which prohibit certain mandatory arbitration clauses in consumer financial products and services contracts.[29] Retail consumers will almost certainly argue that they lack the knowledge or sophistication to create, fully understand, or assent to certain smart contract terms. Arguments concerning knowledge and sophistication may be even more powerful when the code itself forms the contract. Certain retail customers will likely claim that courts should not hold them to included terms or enforcement mechanisms. In all, it seems unlikely that parties, especially retail consumers, will have no recourse with respect to smart contracts in the court system.

Lawmakers and courts will also need to decide how to introduce, authenticate and admit evidence concerning blockchain transactions. The State of Vermont has passed H. 868, which addresses the validity and admissibility of, and presumptions relating to, records created with blockchain technology. The new law provides that extrinsic evidence of authenticity as a condition precedent to admissibility in a Vermont court would not be required for a record maintained by a valid application of blockchain technology, and it establishes a rebuttable presumption of admissibility and authenticity as to basic information, such as the parties and provisions of the smart contract.[30] Without commenting on the strengths and weaknesses of the Vermont law, the law would benefit from courts and arbitration forums adopting uniform standards for using ledger-related evidence in the course of disputes.

Compliance with Regulatory Requirements

At this early stage, legislators and regulators have focused on identifying regulatory measures that may be necessary to mitigate concerns over security, consumer protection and financial crime.[31] To date, various federal agencies have explored digital currencies, and some, such as the Consumer Financial Protection Bureau (CFPB), have issued warnings about the use of digital currencies,[32] but none have yet specifically addressed smart contracts. Further, New York is the first state in the United States to establish a framework for licensing and regulation of businesses engaged in activities related to digital currencies.[33] Any entity subject to New York's digital currency business activity license requirement must also comply with various conditions of conventional financial services regulation, including bookkeeping[34] and anti-money laundering (AML) systems and controls.[35]

Such requirements pose novel legal questions and compliance concerns for users of smart contracts. For example, New York law concerning digital currency business activity were to include users of smart contracts, users may face some difficulty initially complying with the requirement that they maintain books and records of regulated transactions for seven years, including a ledger of all such transactions and the "names, account numbers, and physical addresses" of the parties to the transaction.[36] Compliance with this requirement could be difficult, if not impossible, using a public blockchain, but may be feasible using a private blockchain with a greater deal of control and less anonymity.

In addition, certain fundamental legal concepts, such as the possession of an instrument, may need to be reimagined due to a smart contract's existence essentially as executable computer code that is run on a network. Instead of focusing on the physical possession of an instrument or other contract, regulators and smart contract users may need to establish bounds for ledger-hosted registers on a server or code a smart contract that could be recorded on a blockchain application as a transaction.

Regulator Access and Visibility

As blockchains and smart contracts integrate into industry and become more common, regulators will have the ability to access and see detailed transactional data on a larger scale and in a shorter amount of time. Lawmakers and regulators will need to determine how much data regulators can access as well as how and when they will see it.

Privacy and cybersecurity are major concerns for regulators and industry leaders.[37] To enforce distributed ledger and smart contract regulations, regulators will need varying levels of access to oftentimes private information to monitor and regulate underlying transactions. Depending on the level of access necessary, market participants will likely voice demand for the protection of their information, both from other commercial parties as well as from inappropriate access by hackers or other unauthorized third parties. Commentators suggest that the use of a blockchain for "trade reconciliation, settlement and the like would require sophisticated privacy controls and the management of access to the information residing in the blockchain."[38]

Blockchain programming already allows varying levels of partitioned access to the data within a chain.[39] Further, the use of a permissioned network—as opposed to a public (or permissionless) one—can restrict the data sharing to those entities using the network and the regulators monitoring it. Regulators and the public may also benefit from many inherent characteristics of blockchains and smart contracts. In situations of complicated, legally tenuous, or particularly risky transactions or contracts, the regulator could serve as an advisor by approving contracts, or possibly even coding regulator-approved ones, for industry distribution.

Expanding on the role regulators can play in identity monitoring, KYC regulations in the financial services industry often require the expenditure of vast resources before an entity will transact with a particular client.[4] A blockchain identity issued by the regulatory agency can serve as a trusted KYC compliance shortcut to be used by each entity on the network and each party to a smart contract.[41] Further, prospective parties in subsequent transactions can choose to rely on the identities to inform themselves of other parties' contracting histories.

Regulator Access and Visibility

Finally, regulators may more easily accomplish their auditing and administrative tasks due to the increased access and visibility associated with blockchain technology and smart contracts. Instead of demanding costly reports of transactions from each transacting entity, regulators could have instant, real-time access to the transactions as they take place along with access to an immutable audit trail—all at little to no expense to the contracting parties.[42] However, regulators acting in these roles will not be able to do so in a vacuum.

Regulators will need access to transactional information just as they always have, including the identities, interests and positions of the parties and the values of the transactions. Information aiding in the enforcement of some of the most difficult regulations—such as consistent and truthful recordkeeping—might not be as necessary with an automatic and perfected distributed ledger; trust in the system, however, may demand a peek behind the proverbial curtain and a deep look into the source code of the proffered ledger-hosted contract.

Although demands on manpower could be lessened with the advent of a smart contract, and the burdens of enforcement shifted to the code itself, regulatory oversight will likely always be necessary.[43] Interpretation and approval of a blockchain and smart contract code will require a new regulatory approach and skillset. Industry cooperation will be more important than ever, but a successful integration of reasonable regulation and ledger-hosted smart contracts could provide both regulators and participants alike with significant efficiencies in compliance.

If regulators do require access to code, it will not be the first time. In October 2016, the U.S. Commodities Futures Trading Commission (CFTC) announced that it intends to require automated trading firms to give the CFTC access to their source code (the human-readable part of software) under a proposed market stability rule.[44] Going forward with smart contracts, relevant regulators will also likely require access to code and need sufficient expertise to review it.

References

[1] Nick Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996.

[2] 15 U.S.C. §§ 7001-7006 (2016).

[3] *See, e.g.,* TEX. BUS. & COM. CODE Chapter 43 for the Texas implementation of UETA.

[4] *See, e.g.,* N.Y. Dep't of Fin. Servs. Gen. Couns. Op., *RE: Electronic Signatures on insurance applications and electronic recordkeeping* (Feb. 22, 2007), http://www.dfs.ny.gov/insurance/ogco2007/rg070220.htm (approving electronic signatures by auto insurance applicants and insurance agents maintaining records in electronic format).

[5] *Responsible Innovation*, OFFICE OF COMPTROLLER OF THE CURRENCY, https://www.occ.gov/topics/bank-operations/innovation/index-innovation.html (last visited Nov. 1, 2016).

[6] Consumer Fin. Prot. Bureau, Project Catalyst Report: Promoting Consumer-Friendly Innovation (Oct. 2016), http://s3.amazonaws.com/files.consumerfinance.gov/f/documents/102016_cfpb_Project_Catalyst_Report.pdf.

[7] Howard Schneider, *Fed's Brainard Sees Blockchain as Revolutionary, But Still to Prove Itself*, REUTERS (Oct. 7, 2016, 6:54 PM), http://www.reuters.com/article/us-usa-fed-brainard-idUSKCN1272BG.

[8] *See, e.g., Hill v. Gateway 2000, Inc.,* 105 F.3d 1147, 1150 (7th Cir. 1997).

[9] *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004).

[10] *Id.*

[11] *Ticketmaster Corp. v. Tickets.com, Inc.,* No. CV-997654, 2003 WL 21406289 (C.D. Cal. Mar. 27, 2000).

[12] *Schnabel v. Trilegiant Corp.*, 697 F.3d 110, 121–22 (2d Cir. 2012).

[13] *Corinthian Pharm. Sys., Inc. v. Lederle Labs.,* 724 F. Supp. 605, 610 (S.D. Ind. 1989).

[14] *State Farm Mut. Auto. Ins. Co. v. Bockhorst,* 453 F.2d 533 (10th Cir. 1972). The court also emphasized the human element of the policy reinstatement: "The computerized reinstatement of the policy was not unavoidable as State Farm alleges." *Id.*

[15] *S.E.C. v. Pasternak,* 561 F.Supp.2d 459, 482 (D.N.J. 2008).

References

[16] *See, e.g., id.* at 517 (refusing to find violative conduct involving trades which included limit orders); *Newton v. Merrill, Lynch, Pierce, Fenner & Smith, Inc.,* 135 F.3d 266, 269 (3d Cir. 1998) (addressing claims that limit orders were not executed properly by defendants).

[17] *See* Rick Huckstep, *What Does the Future Hold for Blockchain and Insurance?* DAILY FINTECH (Jan. 14, 2016), https://dailyfintech.com/2016/01/14/what-does-the-future-hold-for-blockchain-and-insurance/.

[18] Smart contract pioneer Nick Szabo discusses escrow and other similar early use cases in his seminal article, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY 9 (Sept. 1, 1997), http://firstmonday.org/ojs/index.php/fm/article/view/548/469#Contemporary.

[19] *See* John Ream, Yang Chu and David Schatsky, *Upgrading Blockchains: Smart Contract Use Cases in Industry,* DELOITTE UNIVERSITY PRESS (Jun. 8, 2016), http://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/using-blockchain-for-smart-contracts.html, at n. 3.

[20] *See generally, Connect Your Smart Contract to the Data Feeds, Internal IT and Payment Methods They Require,* SMART CONTRACT, http://about.smartcontract.com (last visited Nov. 1, 2016).

[21] Evan Weinberger, *'Smart Contracts' Won't Eliminate Need For Lawyers*, LAW360 (Apr. 6, 2015, 6:46 PM), http://www.law360.com/articles/637833/smart-contracts-won-t-eliminate-need-for-lawyers.

[22] Richard Howlett, *A Lawyer's Perspective: Can Smart Contracts Exist Outside the Legal Structure*, BITCOIN MAGAZINE (July 11, 2016, 6:52 PM), https://bitcoinmagazine.com/articles/a-lawyer-s-perspective-can-smart-contracts-exist-outside-the-legal-structure-1468263134.

[23] Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015).

[24] *Burnside-Ott Aviation Training Center v. Dalton,* 107 F.3d 854 (Fed. Cir. 1997) (citing *Commodity Futures Trading Com'n v. Schor,* 478 U.S. 833, 848 (1986)) (analyzing public policy concerns associated with waiving review of contract disputes in narrow context of government contracts).

[25] *See, e.g., Van Duren v. Rzasa-Ormes,* 926 A.2d 372, *aff'd*, 948 A.2d 1285 (N.J. 2008) (whereby the court considered the sophistication of the parties and their relatively equal bargaining positions and whether each was represented by counsel in executing the agreement).

References

[26] *See, e.g., Tabbane v. Switzerland* App. No. 41069/12, Eur. Ct. H.R. (Mar. 1, 2016), *available at* http://hudoc.echr.coe.int/eng?i=001-161870#{"itemid":["001-161870"]} (upholding clauses which state that the decision in arbitration shall be final and binding and neither party shall have any right to appeal such decision to any court of law).

[27] 563 U.S. 333 (2011).

[28] In *AT&T*, the California law sought to protect consumers in suits that predictably involves small amounts of damages, and where the party with superior bargaining power had carried out a scheme to deliberately cheat large numbers of consumers out of individually small sums of money. *Id*. at 339-40.

[29] CFPB Proposed Rule on Arbitration Agreements, 12 C.F.R. 1040 (proposed May 3, 2016), *available at* http://files.consumerfinance.gov/f/documents/CFPB_Arbitration_Agreements_Notice_of_Proposed_Rulemaking.pdf, at 285. The proposed rules seek to prohibit certain pre-dispute clauses which prohibit consumers from joining or pursuing a class action in court—a mechanism seen as essential for obtaining relief where a claim is of minimal monetary value.

[30] The Vermont Bill is available at http://legislature.vermont.gov/assets/Documents/2016/Docs/ACTS/ACT157/ACT157%20Act%20Summary.pdf, Sect I.1 Blockchain Technology

[31] *See generally,* EDWARD V. MURPHY, M. MAUREEN MURPHY & MICHAEL V. SEITZINGER, CONG. RESEARCH SERV., BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES (2015), *available at* https://www.fas.org/sgp/crs/misc/R43339.pdf (last visited Nov. 1, 2016); NORTON ROSE FULBRIGHT US LLP, *Chapter 6: Regulation of Cryptocurrencies,* in DECIPHERING CRYPTOCURRENCIES 14–16 (May 2016) (analyzing cryptocurrency regulation at the federal and state level in the United States), *available at* http://www.nortonrosefulbright.com/knowledge/publications/139847/a-global-legal-and-regulatory-guide-to-cryptocurrencies-chapter-6 (last visited Nov. 1, 2016).

[32] Consumer Fin. Prot. Bureau, *Risks to Consumers Posed by Virtual Currencies* (Aug. 2014), *available at* http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf. (last visited Nov. 1, 2016).

[33] See N.Y. COMP. CODES R. & REGS. tit. 23, § 200 *et seq.* (2015).

[34] *Id.* § 200.12(a).

[35] *Id.* § 200.15.

[36] *Id.* § 200.12(a)(1)–(2). Currently, New York law exempts "merchants and consumers that utilize virtual currency solely for the purchase or sale of goods or services or for investment purposes "from virtual currency business activity license requirements. *Id.* § 200.3 (c)(2)

References

[37] Cliff Moyce, *How Blockchain Can Revolutionize Regulatory Compliance*, CORPORATE COMPLIANCE INSIGHTS (Aug. 10, 2016), http://corporatecomplianceinsights.com/blockchain-regulatory-compliance/.

[38] *Id.*

[39] *See* Stephen Joyce, *Regulators Show Interest in Blockchain to Monitor Systemic Risk,* BLOOMBERG LAW (December 3, 2015), http://www.bna.com/regulators-show-interest-n57982064247/.

[40] Moyce, *supra* note 38.

[41] *Id.*

[42] Moyce, *supra* note 38; *See also* Patrick, *supra* note 37; Joyce, *supra* note 40.

[43] Joyce Hanson, *CFTC Won't Ditch Plan Allowing It To Peek At Trading Code,* LAW360 (Oct. 19, 2016, 5:23 PM), https://www.law360.com/securities/articles/853308/cftc-won-t-ditch-plan-allowing-it-to-peek-at-trading-code.

[44] German regulators see an ever present need for regulator supervision. *See* Ben Cole, *Blockchain compliance raises questions of regulatory scope, intent*, TECH TARGET (May 2016), http://searchcompliance.techtarget.com/feature/Blockchain-compliance-raises-questions-of-regulatory-scope-intent (last visited Nov. 1, 2016).

CHAMBER OF DIGITAL COMMERCE

Working Groups and Initiatives

BLOCKCHAIN ALLIANCE

CANADIAN BLOCKCHAIN POLICY GROUP

STATE WORKING GROUP

DC BLOCKCHAIN CENTER

DIGITAL ASSETS ACCOUNTING CONSORTIUM

GLOBAL BLOCKCHAIN FORUM

SMART CONTRACTS ALLIANCE

CHAMBER OF DIGITAL COMMERCE

www.digitalchamber.org