NORTON ROSE FULBRIGHT

Smart contracts in insurance: Making sense of the terminology and developing use cases

Smart contracts in insurance: Making sense of the terminology and developing use cases[1]

by Ronald D. Smith, Sue Ross and Carey Child with Norton Rose Fulbright; and
Wendy Callaghan, American International Group, Inc.[2]

I. Introduction

For several years, as cryptocurrency prices have periodically surged and pulled back, steady growth of interest in Blockchain, distributed ledgers, and smart contracts has been unmistakable. Still, many observers have noted that there is no consensus about what a smart contract is (including whether one must involve Blockchain at all) and what the term actually means. Despite the ever-increasing discussion of smart contracts, many continue to search for real uses and to question whether there will be widespread adoption.

This article will attempt to make sense of what a smart contract is and provide clear, descriptive, and accurate terminology for smart contracts, with a focus on the insurance industry. It argues that smart contracts make real sense, have real uses, will lead to real change in the insurance industry, and can likely be enforced under existing law.

We will begin with a brief discussion of distributed ledger technologies, including Blockchain technology, and their benefits. We will move on to provide a detailed discussion of the term "smart contract," providing insight into the many ways the term is being used and suggestions on how to improve or synthesize the terminology. We will conclude with a discussion of potential uses for smart contracts in the insurance industry and a look at key issues ahead.

II. Blockchain basics

At its most basic level, a Blockchain is a ledger in digital form. It is created via software shared by cooperating but unaffiliated and untrusting "nodes" (participating computers) that agree (achieve a consensus) on the state of a set of transactions, contained in a "block." Each block is linked to the preceding block to make a chain back to the start. Each node has its own copy of the list of blocks, but transactions can only be performed on the sub-set of Blockchain assets or records for which one has the correct cryptographic key (part of a public/private key pair). Similarly, the technology uses cryptographic tools to make it nearly impossible to alter existing data.[3]

Blockchains are included in a broader group of technologies referred to as distributed ledgers. In fact, while the terms are sometimes used interchangeably, Blockchains are a specific type of distributed ledger. Distributed ledgers generally refer to a shared database, for which an identical copies of which are held on numerous computers. Distributed ledger technology, for example, does not necessarily use a consensus model — it can use a central administrator instead.

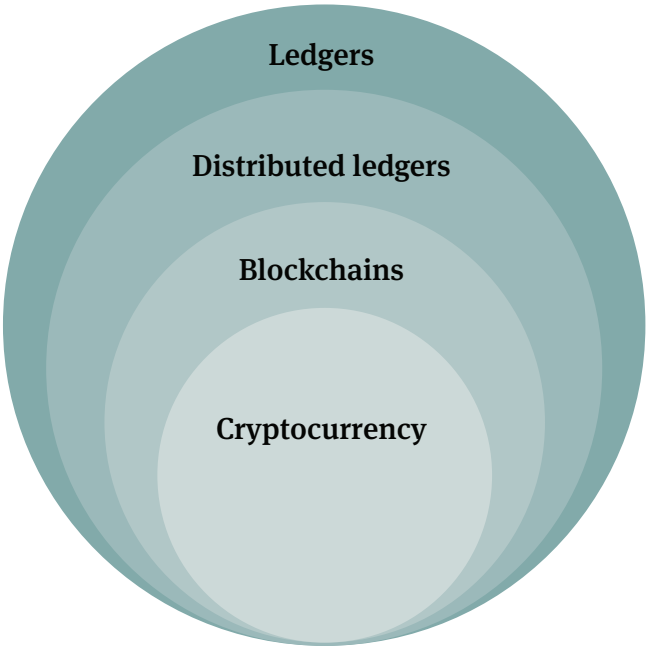
1 This paper builds on a number of other publications developed by Norton Rose Fulbright. For further reading on the subject of smart contracts, please see Smart Contracts: coding the fine print (available at http://www.nortonrosefulbright.com/knowledge/publications/137955/smart-contracts-coding-the-fine-print); Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright White Paper (available at http://www.nortonrosefulbright.com/files/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf); Unlocking the Blockchain: Chapter 2: digitizing the insurance value chain (available at http://www.nortonrosefulbright.com/knowledge/publications/147676/unlocking-the-blockchain-digitizing-the-insurance-value-chain-chapter-2).

2 The authors would like to thank Rajika Bhasin, Associate General Counsel, AIG, as well as Tori Payne, Erin Berkowitz and Jean-Baptiste Pessey for their significant assistance. The views expressed in the article are those of the authors and are not meant to reflect the views of American International Group, Inc. or its affiliated companies.

3 This technology relies upon the cryptographic hash function, which is a mathematical way of taking input data (numbers or letters or both) and scrambling it, for a result or "digest" that is a certain number of characters in length. An example would be if the word "fox" were hashed to a 40-character digest, the result could be DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17. Hashing the sentence "the red fox jumps over the blue dog" would also yield 40 characters but would look very different: 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC. Even changing one character in the input can lead to a very different result: changing the "v" in "over" to a "u" would result in: 8FD8 7558 7851 4F32 D1C6 76B1 79A9 ODA4 AFE 4819. The hash function can be used to verify that some specific input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value (a one-way trapdoor). Hashing is put to a variety of uses in Blockchain, including assuring integrity of transmitted data.

Blockchain is a form of DLT

Figure 1



Blockchains can be private or public, and permissioned or permissionless. A public, permissionless Blockchain allows any computer to participate; an example is Bitcoin. A private, permissioned Blockchain would permit only certain computers that are approved by the administrator to access the transactions and transact on the network (Ripple is often cited as an example of such a network).

Blockchains and distributed ledger technology can offer significant benefits that include

A single replicated ledger. Participants do not have to maintain their own separate records or reconcile them if differences occur (through error, fraud, etc.). Instead, the same ledger is agreed upon and replicated across participants to serve as the single source of truth.

Creating new platforms. Blockchain and distributed ledgers allow users to simplify and reengineer business processes without the need for traditional centralized vetting of information. The resulting platforms can utilize data from internet of things (IoT) devices and many other sources to transact business.

Replicated recording of the time and specifics of each transaction. Once consensus is achieved, all nodes have the same information at the same time and all nodes "see" the transaction at the same time.

Speeding transfers of value and settlements. Because all nodes have access to the same information at the same time, transactions and settlements between participants can generally take place quickly and frequently without the need for a third party. Many have referred to the potential "disintermediation" of third parties, and resulting efficiencies, as a major benefit of Blockchain technology.

Increased security and authenticity of data. As discussed above, cryptography protections (public/private keys and hash functions) are built in. Furthermore, it is becoming increasingly popular not to store the entire transaction record in a block but rather only a summary or "pointer block" that points to where the data resides off a Blockchain.

Sharing costs. Many current practices, for tasks like collecting client data for know your customer (KYC) and onboarding, are redundant and complicated. Organizations can use Blockchain and distributed ledger technology to share costs for redundant tasks and, as a result, reduce costs. Note that privacy concerns may keep KYC data "off-chain."

No single point of failure. Blockchains are typically designed so that there is no one central authority, although other forms of distributed ledger technology may use a central administrator. As a result, with a typical Blockchain, if one or even several nodes are not available, the Blockchain continues to record transactions in the intended fashion.

Smart contracts can leverage Blockchain and distributed ledger technology to automate specified agreed upon functions, as described below.

III. Smart contracts

Before going into the details of smart contract terminology, it is important to consider why so many see great potential for smart contracts being combined with Blockchain technology. While the next few sections will detail how many use the term "smart contract" to refer to a wide range of scenarios, what are the potential benefits of smart contracts?

As an illustration, consider a typical breach of contract dispute. Some of the most important elements to demonstrate seem simple in the abstract but can be complex in reality. Parties can spend inordinate amounts of time and money arguing about what the terms of an agreement are, who agreed to them, and when they agreed to them. By entering into agreements on a Blockchain, there will be shared and immutable proof of an agreement's terms, the parties' consent to the terms, and the time of the agreement. While we do not anticipate that smart contracts will resolve all ambiguity or end contract disputes, they have the potential to narrow contested issues and reduce ambiguity in a significant way.

Beyond offering a shared, hashed record of many important facts surrounding the making of an agreement, smart contracts also offer important advancements in the realm of performance. Specifically, when the terms of a contract are satisfied by performance, Blockchain technology can automatically transfer payment promised in exchange for performance, leaving a record of payment.

III(A). What is a smart contract?

To developers and others working directly with Blockchain technology, the term "smart contract" is most often used to refer to a certain type of software program and the code of which it is comprised. Specifically, they use the term to refer to a software program recorded on the Blockchain, which itself controls Blockchain assets and is executed on the Blockchain. The term is widely used in this sense with respect to Ethereum, a Blockchain platform specifically designed for deployment of smart contract programs.

To business people and lawyers, the term "smart contract" often means an actual legal contract that is automated, replicated or replaced in whole or in part through use of Blockchain technology. These smart legal contracts can be a combination of smart contract code and more traditional legal language; accordingly, they do not need not to be entirely in smart contract code.

In both scenarios, the term "smart contract" can refer to either a "pure" smart contract, where there is a self-executing promise expressed in code, or a "partly" smart contract, where certain elements such as enforcement are automated but other elements, such as the other terms of an agreement, are expressed in natural language. Making things potentially more confusing, some have used the term "smart contract" in a much more informal manner, where there may be no promises, no counterparty, no agreement, and potentially no automated performance.

III(B). Examples of the uses of the term "smart contract"

In this article, our intention is not to take sides or put forth what we contend should be the definitive definition of a smart contract. Instead, begin with an analogy to the electromagnetic spectrum of infra-red, visible light, and ultra-violet to: (1) show the place of smart contracts within the spectrum of certain related technologies; and then (2) focus on different variations of smart contracts ranging from partial automation of contract functions, to partly smart contracts, to "pure" smart contracts. We then discuss some examples, and whether they are smart contracts.

Similar to other areas of specialization in the Blockchain industry, a consortium has been created relating to smart contracts: the Accord Project. The Accord Project has created an open source protocol for the formation and execution of smart legal contracts that is designed to be a Blockchain-agnostic standard implementation, including a domain-specific language, execution engine, and templating system.

III(C). Are smart contracts enforceable under current law?

i. In the United States

Multiple writers have already commented on how smart contracting fits within existing US contract law. For instance, one article strongly argues that existing laws, including the federal Electronic Signatures in Global and National Commerce Act ("ESIGN") and the Uniform Electronic Transaction Act ("UETA") "already allow for smart contracts

Figure 2

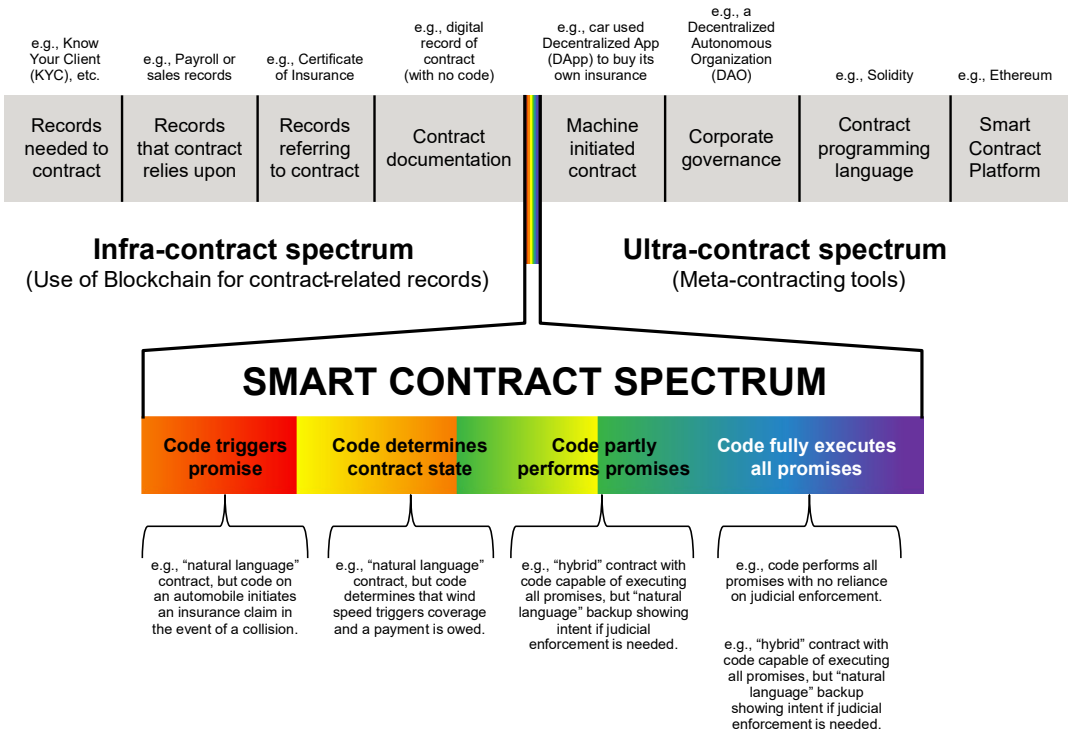


Table 1

Might be called a "smart contract"	Is it a smart contract?
Code: "if a Cat 4 hurricane is reported in Florida, then [specified payment] is [automatically, by the code] released from escrow"	**Pure Smart contract.** Promise, expressed in code, self-executing.
Natural language contract providing for the payment of [specified amount] if a Cat 4 hurricane hits Florida, and further provides for code that will automatically release that payment from escrow if such a condition is reported.	**(Partly) Smart contract.** Although the promise is first expressed in "natural language," enforcement is at least partly automated (and so the promise is also expressed in code).
Code: "if there is no milk in Alice's smart refrigerator, text Alice that she needs to buy milk [automatically, by code]."	**Not a smart contract / informal reference.** Although expressed in code and self-executing, it does not involve promises. It instead addresses administrative rights. This might be an example of what is more correctly called a Decentralized Application ("DApp"), or part of a Decentralized Autonomous Organization ("DAO"), which can be created using some of the same tools and platforms as are used by smart contracts. As the name implies, DApps are similar to "apps" in that they are applications, but they typically are peer-to-peer rather than running on a single computer. DApps can run on Blockchains, and in some cases may be able to enter into smart contracts. DAOs generally control some kind of internal property that is valuable in some way, and the DAO has the ability to use that property as a mechanism for rewarding certain activities, including via smart contracts.

to be enforced."[4] Noting that ESIGN and UETA contain provisions that put electronic signatures on equal footing with physical ones, the authors conclude that the use of cryptographic keys to sign and acknowledge contracts will constitute electronic signatures under both ESIGN and UETA.[5]

At a more fundamental level, it should not be surprising that commentators generally agree that the same legal requirements will be applied in enforcing (or not enforcing) traditional contracts and smart contracts.[6] Indeed, ESIGN states that "a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[7] UETA contains similar language.[8] Accordingly, the focus of ESIGN and UETA is not to create some new body of contract law. Rather, the point is to make sure that courts afford the same respect and treatment to electronic contracts, electronic signatures, and electronic records that they afford traditional agreements with wet signatures.

ii. In non-US jurisdictions

Whether smart contracts can give rise to legally binding contractual relations under the laws of non-US jurisdictions varies significantly depending on the jurisdiction. There are, however, some common themes.

The electronic nature of contracting is unlikely to be problematic for many (but not all) jurisdictions in relation to establishing contractual formation. In the European Union, Article 9 of the Electronic Commerce Directive (which applies on both a B2B and B2C basis) requires member states of the European Union (which currently include the United Kingdom) to ensure that their legal systems allow contracts to be concluded by electronic means. Further, it requires that legal requirements applicable to the contractual process do not create obstacles for the use of electronic contracts or result in such contracts being deprived of their legal effectiveness on account of their having been made by electronic means.

Australia, South Africa and China have gone so far as to put in place legislation to clarify aspects of contract formation in relation to electronic contracting which is very helpful in analyzing the legal status of smart contracts.

The common law in a number of countries has applied existing principles in analyzing electronic transactions by email and other means. Many jurisdictions view certainty as to what constitutes contractual terms (and whether they are comprehensive enough) as a critical factor necessary to establish the formation of a legally binding contract. However, smart contracts that purely digitize a particular process but do not include, or operate in conjunction with, contractual terms (express or implied) may not satisfy such requirements. In some cases, other quite technical requirements of the applicable jurisdiction's law (typically prescribed by legislation) may be an impediment to rolling out smart contracts that are intended to have legally binding contractual effect. For example, in the United Kingdom, certain agreements are required to be executed as a deed. In other European Union jurisdictions, certain agreements are required to be notarized.

Under English law, the usual rules relating to contract formation will probably apply to determine the legal status of a smart contract. Whether a particular smart contract gives rise to a legally binding contractual arrangement under English law may turn in part on the type of smart contract at issue and the factual matrix within which it operates. The fact that a contract may be wholly electronic is unlikely to determine the outcome.

iii. Looking ahead

Commentators have also noted that smart contracts, given their automated performance, will introduce new challenges.[9] Generally speaking, automated performance that cannot be stopped by the parties may alter the leverage of the parties in a dispute and lead to more contract disputes seeking to undo performance instead of suing for failure to perform.[10]

4 Alan Cohn et al., *Smart After All: Blockchain*, Smart Contracts, Parametric Insurance, and *Smart Energy Grids*, 1 GEO. L. TECH. REV. 273, 285 (2017).
5 *Id*. at 288-290.
6 Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 326 (2017) ("the issues of contract formation are largely the same in the traditional and smart contract world.") (referred to hereinafter as "*Law and Legality*"); Kevin Werback & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 368 (2017) ("At a basic level, a smart contract can meet the legal requirements for a valid and enforceable common law contract: offer, acceptance, consideration, capacity, and legality.") (referred to hereinafter as "*Contracts ex Machina*").
7 15 U.S.C. § 7001(a)(1).
8 UETA specifies that electronic records, electronic signatures, and contracts in electronic form "may not be denied legal effect or enforceability" based on their electronic nature. UETA at § 7.
9 It has been observed that smart contracts enable individuals to construct their own systems of rules creating "order without law and implement[ing] what can be thought of as private regulator frameworks ...." Blockchain and the Law: The Rule of Code, Primavera De Filippi and Aaron Wright, at 5. Di Filippi and Wright term this concept "*lex cryptographica*."
10 Law and Legality at 322; Contracts ex Machina at 370.

In other words, in a traditional setting, if a party to a contract wanted to claim that no enforceable contract existed, the party could simply withhold payment (or other performance), requiring the other party to bring an action for alleged breach. If smart contract code resulted in automatic performance of the same allegedly unenforceable agreement, the code would still trigger payment, forcing the same party to bring suit to have its money returned. Accordingly, courts or arbitration bodies would need to hash out issues like mutual intent, consideration, and capacity *after the fact* because smart contract code may press forward even if it violates some aspect of controlling contract law.[11]

While there may be initial challenges, we also expect that information held on a Blockchain (or pointed to off-chain) will be admitted by courts as evidence under the business records hearsay exception, and potentially other avenues. One recent law review article succinctly argues that "Blockchain receipts and the consensus algorithm are quintessential examples of record-keeping in the ordinary course of business."[12] Further, individual states have enacted legislation aimed at making it easier to admit evidence created with Blockchain technology. For example, in 2016, the state of Vermont enacted a law on validity and admissibility of, and presumptions relating to, records created with Blockchain technology.[13] The law states that a digital record that is electronically registered on a Blockchain shall be deemed to be "self-authenticating," and can be a "business record" for purposes of Vermont's rules of evidence.

IV. Use cases in the insurance industry

IV(A). Blockchain and distributed ledger technologies

By one estimate, DLT "could reduce banks'" infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between **US$15bn to US$20bn per annum** by 2022."[14] That is significant savings.

Are there similar savings applicable to the insurance and reinsurance industries?

Here is how Blythe Masters, former JP Morgan managing director and now CEO of Digital Asset Holdings LLC, explains the potential for DLT:

> "[W]hen multiple parties to a common transaction interact, they are inclined to keep their own separate records of their respective piece of a joint transaction, and that leads to tremendous inefficiencies. An enormous amount of time, particularly but not limited to financial services, is spent reconciling the differences between records kept in distinct databases that ultimately refer to the same transaction between two parties."[15]

These databases of transaction records are sometimes called "ledgers" or the "books and records" of a market participant. The fact that a single transaction can result in the need to reconcile multiple ledgers, held by multiple market participants, results in duplicated efforts, errors and inconsistencies, and ultimately billions of dollars in time and money spent reconciling and auditing (and in some cases litigating about) those ledgers.

The insurance and reinsurance industries exhibit all of these challenges. As illustrated below, the insurance and reinsurance risk-transfer process is complex and involves many parties. There are many other entities that might need to access, or reconcile, various ledgers held by market participants:

In this context, consider the following issues surrounding a single workers' compensation insurance policy

- Prior to inception of the policy, the insured will need to satisfy KYC requirements of the insurer, and will also prepare an insurance application. The associated documentation will be submitted to the broker, and then by the broker to the insurer (likely multiple insurers).

11 Law and Legality at 322-329; Contracts ex Machina at 367-374.
12 Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI.-KENT J. INTELL. PROP. 440, 448 (2017). The same article also argues that Blockchain evidence may bypass hearsay rules entirely because they are "computer-generated evidence." *Id.* at 446-48. *See also* ARIZ. REV. STAT. § 44-7061 (signatures and records secured through Blockchain technology; smart contracts; ownership of information; definitions), and TENN. CODE ANN. §§ 47-201-47-202 (similar to Arizona, and defines a "smart contract" as "an event-driven program, that runs on a distributed, decentralized, shared, and replicated ledger and that can take custody over and instruct transfer of assets on that ledger.").
13 12 V.S.A. § 1913.
14 *The Fintech 2.0 Paper: Rebooting Financial Services* available at http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf (emphasis added).
15 Interview with *Wall Street Journal* (Jun 19, 2016) available at https://www.wsj.com/articles/what-blockchain-is-and-what-it-can-do-1466388185

Figure 3

The insurance and reinsurance risk-transfer chain is complex and involves a large number of participants. This figure shows only participants that are actual risk-transferring or risk-bearing entities.

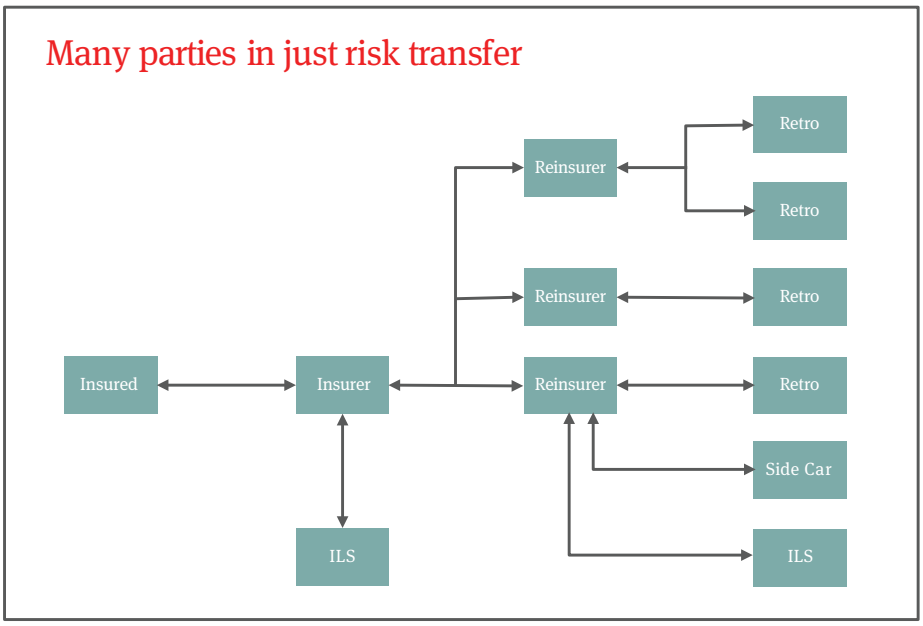


Figure 4

This figure adds multiple intermediaries that facilitate risk-transfer transactions.

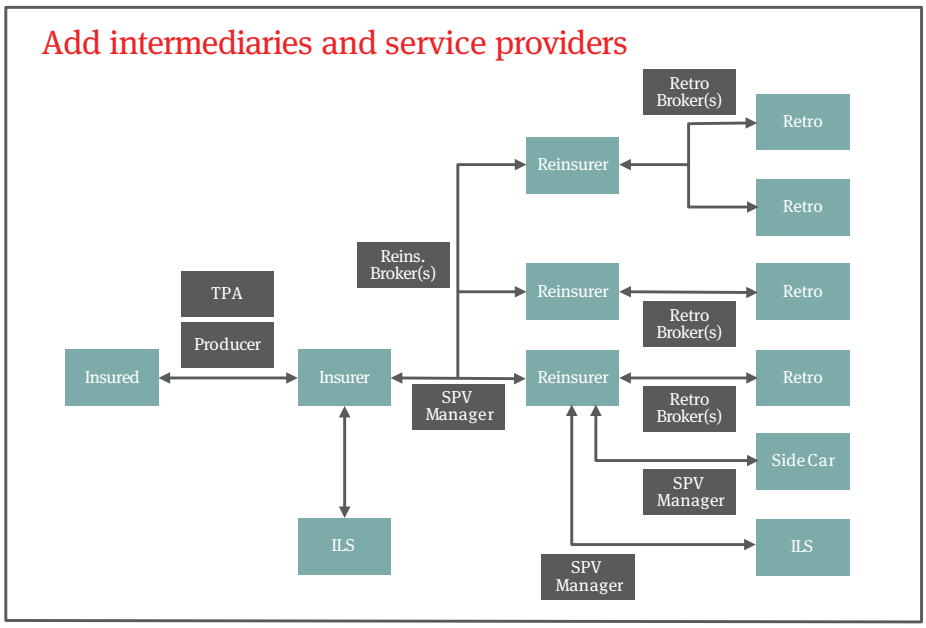


Figure 5

Once KYC requirements, rating agencies, and regulators are added, there can be an impressive number of participants that could need access to information generated in relation to a single insured and policy.

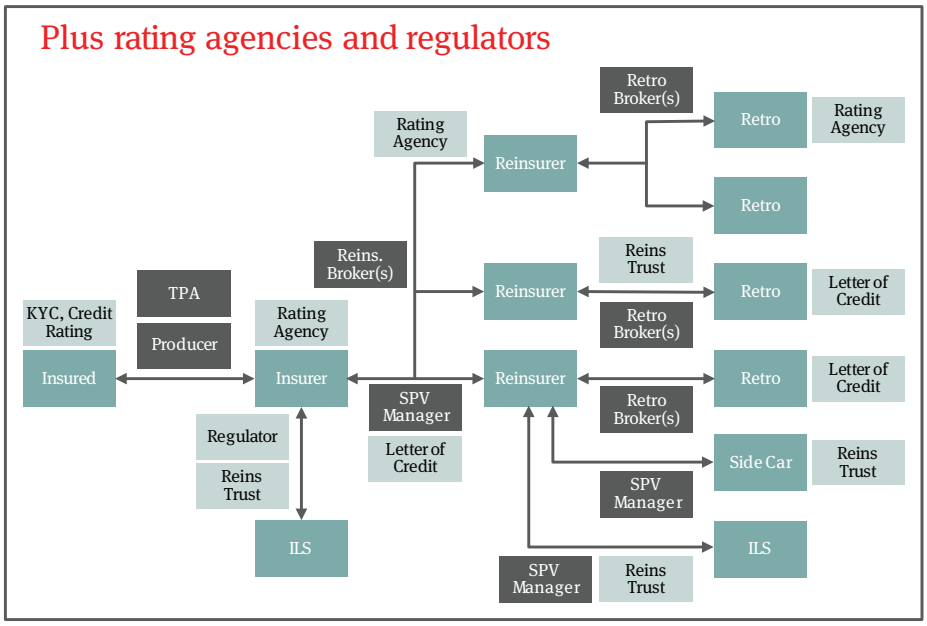
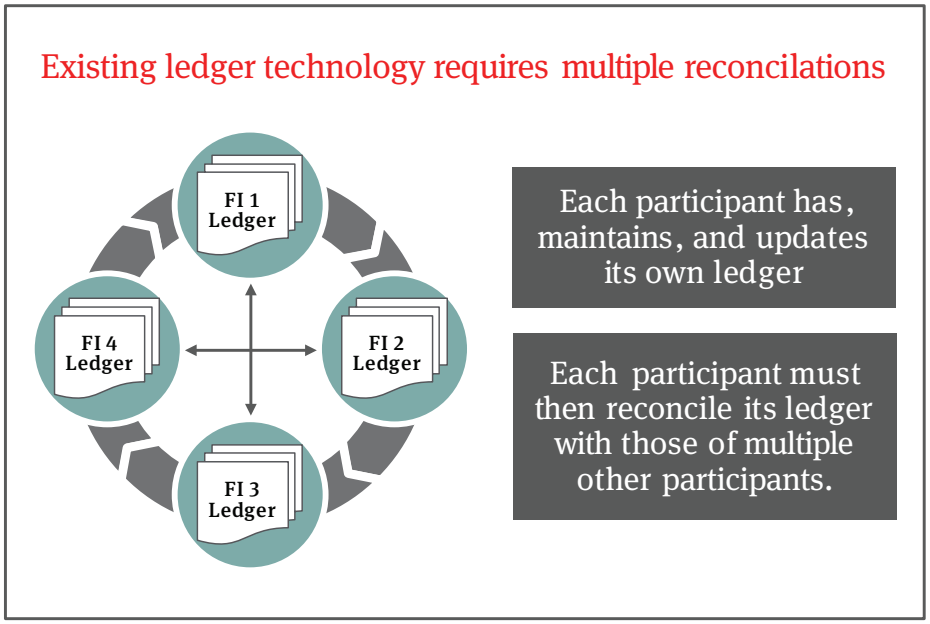


Figure 6

Under existing ledger technology, each participant maintains its own set of records (or ledgers), which brings the potential for errors and differences in records. This results in the need for each of the various parties to reconcile with (and periodically audit) the records of other participants, at great expense in terms of personnel, money, and speed of settlement.



Because the KYC and application might be necessary for regulatory compliance and/or relevant to a subsequent non-disclosure claim, copies (each potentially different) will be kept by the insured, by the broker, and by each insurer that issues a policy. In the event of a dispute, any differences between the records will need to be reconciled. *In a Blockchain environment, this duplicative documentation is replaced with a shared, unalterable record. (As noted above, privacy issues may keep KYC information "off-chain.")*

- Once the policy is issued, the "definitive documentation" of the policy will consist of numerous parts, and many endorsements. During the term, policy terms may be changed by endorsement, or additional insureds added. The insured, the broker, and the various insurers will each have (and have to maintain) their own copy of the policy, and all subsequent endorsements and modifications, which brings the potential for errors and differences in the records. *On a Blockchain, this duplicative documentation is replaced with a shared, hashed record, which can be updated with a complete audit trail of all changes made.*

- During the policy period, the amount of premium and the persons covered may depend upon information kept in the insured's records (e.g. employee lists and payroll). The numbers will be reported through the broker, and by the broker to the insurers. At each step, the numbers will need to be reconciled. One or more insurers may exercise rights to "audit" the insured's ledgers to ensure that payroll or other premium bases are being reported correctly. *In a Blockchain environment, updates to premium can be calculated by a smart contract using code that relies upon or points to on- or off-chain documentation.*

- Regulators, auditors and ratings agencies will require access to the books and records of the insurers, which can be an expensive process that increases the cost and decreases the effectiveness of oversight. *In a Blockchain environment, these entities can be given access to a shared ledger with less friction and greater visibility.*

- Each of the insurers will have its own reinsurance program. The program could consist of multiple types of traditional insurance, as well industry-loss warranty contracts, and insurance-linked securities. In addition to the multiple direct counterparties, each placement will involve brokers and other service providers and intermediaries. Each step will involve the need to document the "placement" information and "definitive documentation" of the terms. In addition, each step will involve calculating premium and recording premium payments. *In a Blockchain environment, smart contracts can directly access a shared ledger, apply contract terms, and determine amounts owed.*

- In the event of a loss, the whole chain of separate ledgers maintained by multiple market participants (including new participants, such as claims adjusters) will again need to be reconciled as part of the claims settlement process. *In a Blockchain environment, settlement of amounts owed can happen quicker, and in some cases may be automatic.*

In short, by moving these processes onto a distributed ledger, all of the market participants will be operating off of the **same** ledger, with the ledger illustrating a consensus representation of the state of affairs between the parties. The time and money currently spent on the duplicative creation and maintenance, and the reconciliation of different ledgers held by multiple market participants can be significantly reduced. The same definitive record could be made of the insurance policy, the reinsurance submission, and the various reinsurance contracts. The basis for the calculation of premium, and the payment of that premium could be documented in a shared ledger, which will also act as confirmation that the insurance was issued for purpose of claims handling. A shared ledger is particularly useful to facilitate transparency through a chain of transactions, as in insurance and reinsurance. The reinsurer, for example, can have visibility to, and can assess the provenance of, the numbers that are used to determine the premium base from which the reinsurance premium is calculated.

None of this necessarily involves smart contracts, process automation, or autonomous agents. Indeed, there are opportunities for the use of each of these technologies regardless of whether Blockchain digital ledger technology is adopted. Nevertheless, operating these technologies utilizing Blockchain technology certainly increases their potential functionality and cost savings.

IV(B). Smart contracts

Examples of potential use cases include automated performance, reinsurance, and eventually agreements written entirely in code.

IV(B)(1). Automated performance

Integrating our discussion of smart contract terminology above, one use case for insurance involves a partly smart contract with automated performance. In a typical situation, an insured would pay premiums to an insurer for coverage. The authoritative policy document would continue to be a natural language agreement between the insured and insurer. However, specified events triggering payment would be placed on the Blockchain. An outside, trusted data provider (or "oracle") would provide information to determine whether and when the specified event took place, triggering payment and reducing many issues in the current claim payment process.

For instance, the oracle could determine when a specified amount of rain has fallen, when wind speeds reached a certain level, when a death has occurred, or when a hospitalization for an injury has occurred. Each would use a partly smart contract to deliver payment quickly. We have already discussed above entirely new chains of distribution that this technology may create, such as autonomous agents, including DApps, on an IoT initiating claims, or buying their own insurance.

The industry has already begun to see this technology put into practice, with flight delay coverage.[16] The policy document is a natural language agreement between the insurer and the passenger. The delay of the flight past a two-hour window, where the airline flight status feed functions as the "oracle," triggers payment to the passenger. Although this example illustrates a very simple insurance policy, the industry is investigating more complex and connected coverages. Indeed, there are currently industry-wide efforts seeking to use distributed ledger technology to create platforms to run insurance value chain transactions.

IV(B)(2). Reinsurance

Within the insurance and reinsurance industries as a whole, reinsurance seems likely to present a highly-attractive testing ground for smart contract technologies.

As shown in the charts above, reinsurance transactions, as traditionally conducted, involve a large number of market participants, and thus a large number of duplicative ledgers that are separately maintained and must be reconciled at great expense. As a result, DLT has significant potential in the reinsurance industry.

Certain aspects of the reinsurance industry are also particularly amenable to testing smart contract technology. Industry-loss warranty contracts and catastrophe bonds, among other projects, have payment provisions that are intended to be triggered based upon objective external parametric criteria. These could be used, for example, with code that would automatically initiate claim, or a reinsurance payment, upon the happening of such a parametric trigger.

IV(B)(3). Agreements entirely in code

The smart contract technology is currently in its very early stages and just beginning to be put into practice. Given the current state of the technology, we are not yet at the point of having insurance agreements written and executed entirely in computer code. The complicated technology appears best suited at this time for transactions between commercial entities (such as large reinsurance agreements) or for the provision of services in the background of consumer transactions (such as the process of checking records to determine if a consumer qualifies for a particular type of coverage). The coding in connected insurance policies could lead to smart contract processes in the future for both commercial entities and consumers.

Because the user interface of smart contract technology is currently not consumer friendly, the solution may be the use of "multi-sig" (multiple-key signature) programming. For example, each of the parties would hold a private key, with a third in escrow or with another trusted third party. The agreement would be written such that any two keys can determine whether a contract condition (such as a reasonable standard) has been met. If both parties agree, they use their two keys and the smart contract executes the appropriate code. If the consumer, for example, loses the key, the escrow key would be used upon the consumer's request to permit the smart contract to execute the code.

16 Maria Terekhova, *AXA turns to smart contracts for flight delay insurance*, *Business Insider*, (Sept. 15, 2017)

IV(C) The path forward

Of course, as with any new technology, getting from an idea with potential to the implementation of that idea will involve surmounting the hurdles. Some of the key challenges are as follows

- **Hard changes:** Many see challenges in the required changes in business processes to integrate with the Blockchain, and then to utilize smart contracts. The insurance industry can at times be conservative and slow to adopt new technology. On the other hand, as both incumbents and potential new entrants recognize the potential cost savings (and corresponding competitive advantage) to adopters, there will be increasing pressure to move forward (or at least not get left behind).

- **Resistance to disintermediation:** Incumbents might be tempted to resist the adoption of technology that disintermediates established players. On the other hand, there will be room for intermediaries that provide added value apart from their position as an intermediaries.

- **Concerns about control:** Network effects in Blockchains raise the potential for abuse should they fall under the control of a small group. Similar questions are being raised with respect to who will control smart contract applications. Insurance agents and brokers worry that they will be disenfranchised because Blockchain and smart contracts may increasingly automate their tasks. For instance, if automobile insurance is purchased by an autonomous agent built into the car, then will the manufacturers be able to extract value because of their control of this process? Insurers are also concerned that third-party oracles that supply information necessary for smart contracts (weather conditions, death certificates, etc.) may charge high fees and adversely affect the economics of policies. Some are raising questions about the reliability of oracles and whether they are adequately protected from tampering. Of course, some types of Blockchain (public permissionless) are designed specifically to avoid the risk of the network being captured. To the extent other types of Blockchain are used, participants and regulators will want to push for them to be as open as possible, and not under the control of incumbents. However, these new technologies are raising the potential for the same types of antitrust and competition issues raised by other disruptive technologies, and if they occur, will need to be addressed using the same tools.

- **Consumer protection:** Regulators may have concerns about enforcing controls on decentralized systems, regulatory ability to audit smart contracts and whether consumers will understand how smart contracts work, how they will receive required notices and, more generally, will consumers be adversely affected? For this reason, we anticipate that consumer facing use cases will — for at least the foreseeable future — be limited to use cases that include natural language contracts, with attention to human-oriented consumer interaction, and that ultimately rely on regulatory and judicial enforcement.

- **Programming errors:** Smart contracts are only smart in the sense that automaton is smart. They will repeatedly follow the same instruction even if it is erroneous. As a result, prudent participants will take an incremental approach in shifting towards smart contracts. For example, early implementations will likely be hybrid contracts in which natural language documentation exists alongside the code to document the parties' intent. This could be paired with the ability in the code for a party to effectively hit a pause button if the smart code contract was not working as intended. If both parties agree, they would revise the code. If they disagree, a dispute resolution mechanism would be activated.

- **Private key management:** Participants must take exceptional care to protect private keys from hacking, avoid losing track of the keys, and prevent unauthorized use. Unlike typical banking credentials, once they are lost, private keys may be unrecoverable.

- **Business model:** The business model of large parts of the insurance industry is based on fractional reserving and investing reserves which is potentially incompatible with a purist version of a smart contract. This may mean that pure smart contracts will be tried first in areas (such as certain types of reinsurance) with a different model. If the cost savings are sufficient, the pure smart contract, fully reserved, may over time work to displace the current business model.

- **Subjective terms:** Pure smart contracts work best when all aspects of the contract are objective. How will terms like "reasonable" and "customary" be interpreted? For some use cases (as discussed above), purely objective criteria are sufficient. Where more subjective terms are required, the solution may be the use of "multi-sig" (multiple-

key signature) programming. For example, each of the parties would hold a private key, with a third in escrow. The contract would be written such that any two keys can determine whether a contract condition (such any reasonable standard) has been met. If both parties agree, they use their two keys and the smart contract executes the appropriate code. If the parties disagree, the escrow key would be given to an arbitrator. Upon making her decision, the arbitrator's key, together with that of the prevailing party, would permit the smart contract to execute the code.

V. Conclusion

Smart contracts (self-executing promises expressed in code) and partly smart contracts (where only certain elements are automated) can lead to real change in the insurance industry. Using the correct terms for true smart contracts and partly smart contracts can help overcome regulatory and enforcement concerns. Insurers should be prepared to address concerns related to smart contracts. Regulators will want to see insurers demonstrating a thorough understanding of the technology, including how programming errors will be addressed.

Although not a silver bullet, smart contract technology has the potential to provide substantial benefits both to insurers and to insureds through faster, more accurate transactions and a shared source of truth. The technology will likely be first approved in commercial transactions, such as reinsurance, especially where the key factors are objectively determined. Once regulators and the industry become comfortable with smart contracts, the technology and its benefits can be extended to consumers.

About the authors

Ronald D. Smith is a partner with Norton Rose Fulbright in Dallas. Wendy Callaghan is chief innovation legal officer and associate general counsel at American International Group, Inc. (AIG) in New York. Sue Ross is Senior Counsel with Norton Rose Fulbright in New York. Carey Child is Senior Counsel with Norton Rose Fulbright in Washington, DC.

Ronald D. Smith
Norton Rose Fulbright
Partner, Dallas

Wendy Callaghan
American International Group, Inc.
Chief Innovation Legal Officer and Associate General Counsel, New York

Susan L. Ross
Norton Rose Fulbright
Senior Counsel, New York

Carey G. Child
Norton Rose Fulbright
Senior Counsel, Washington, DC

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.

NORTON ROSE FULBRIGHT