By Gary L. Johnson

Blockchain Technology and the Insurance Industry

"You can never plan the future by the past."

Edmund Burke, letter to a member of the National Assembly (1791).

In my practice, I have the opportunity to speak with lawyers across the country. I hear, with increasing frequency, their concern at the pace of change that is occurring not just in the legal profession, but also in their client's businesses. The more lawyers understand the changes facing their clients, however, the better prepared we are to help our clients master those transitions.

The purpose of this article is to provide an overview of a change in technology occurring in the insurance industry that, according to some commentators, has the potential to transform radically how insurance policies are marketed, underwritten, and adjusted. The trigger for this transformation is computer based blockchain technology, which is already in limited use in certain areas of the insurance marketplace. A blockchain is a digital database, consisting of individual, linked records ("blocks"). As will be discussed below, each block is timestamped and tied to a previous block. Blockchain technology permits a decentralized, peer-to-peer, method of entry, but with inherent protections against changes to previously entered data. It also facilitates the use of that ledger of data to self-execute instructions and other transactions.

The application of this distributed ledger of transactions, however, can have profound consequences. Blockchain technology is described as adding improved attestation, dramatically lower costs, lighting speed, lower risks, greater innovation of value, and improved adaptability for the investment banking, insurance, accounting and retail banking industries. Don Tapscott and Alex Tapscott, Blockchain Revolution 60–61 (2016)(hereinafter Revolution).

In this analysis, we will first review some current and proposed uses of blockchain technology, and distinguish blockchain technology from other current developments in the legal area. Then, basic blockchain technology, which was essential to the development of Bitcoin, will be examined. Next, we will work through the mechanics of how the use of blockchains promote security, promote privacy, promote transactional compliance by the use of smart contracts, and promote user inclusion into the insurance marketplace. Finally, we will explore potential blockchain use in the insurance industry and how it may expand in the near future.

Blockchain Today

Everledger, founded in 2015, has built a global digital ledger that tracks and protects valuable assets by collecting an asset's defining characteristics, history, and ownership. Everledger began its business with diamonds, using more than 40 characteristics of the gem to create its identification. This information is placed in a permanent record on a blockchain and the digital incarnation is used by various stakeholders to form provenance and verify authenticity. Everledger intends to expand its market by constructing its blockchain database for other high value goods.

A German start-up company called Etherisc developed, using blockchain technology, an app called "Flight Delay," that fully automates the underwriting and payouts of flight insurance policies. It was a limited application test. The customer just enters the flight number and pays a small fee, and if the flight is delayed, the payout is automatically transferred to her or his account through the use of a smart contract. Once this app is deployed and properly configured, it works fully autonomously with no almost interaction or maintenance needed from a claims adjuster. *See* https://etherisc.com/whitepaper.

In October of 2016, five insurers launched "Initiative B3i," which by the spring of 2017 had grown to 15 members. Members of the B3i initiative are collaborating to explore the ability of blockchain technology to increase efficiencies in the exchange of data between reinsurance and insurance companies. The B3i initiative is providing these companies with a platform for the efficient and cutting-edge testing and improvement of inter-company processes and to allow for the development of common standards for the insurance industry. *See* L.S. Howard, Blockchain Insurance Industry Initiative B3i Grows to 15 Members, *Insurance Journal*, February 6, 2017, *available at*

■ Gary L. Johnson is a shareholder and director with Richards Brandt Miller Nelson in Salt Lake City, Utah, where he concentrates his practice on insurance law and catastrophic injury claims. Mr. Johnson is a fellow of the American College of Coverage & Extracontractual Counsel, a former Utah State Representative to DRI (2013–2016), a member of the DRI Insurance Law Committee, and a member of the International Association of Defense Counsel.

http://www.insurancejournal.com. One of the participants in B3i opined that blockchain technology "has the potential to link insurance entities in a powerful data-sharing framework, and the B3i consortium and pilot project can demonstrate and accelerate this innovation." *See* Giulio Prisco, Insurance Giants Generali and RGA Join Blockchain Insurance Industry Initiative B3i, *Bitcoin Magazine*, February 8, 2017, *available at* https://bitcoinmagazine.com.

On April 25, 2017, it was reported in the *Wall Street Journal* that the government of Dubai announced that by 2020, its goal was to conduct a majority of the Emirate's business using blockchain technology, which it expected to make government services more efficient and help promote enterprise in Dubai because it will be easier to do business there. Over the coming months, Dubai will conduct workshops with key government and private organizations to determine which services can best utilize blockchain technology and also to educate the public and private sectors about the technology's potential. Dubai is the first city to attempt to implement blockchain technology on a government level.

In June of 2017, *Reuters* and the *Insurance Journal* reported that AIG partnered with IBM to develop a "smart contract" policy that uses blockchain technology to manage complex international coverage. AIG and IBM completed a pilot of a smart contract multinational policy for Standard Chartered Bank PLC, which the companies stated is the first of its kind using blockchain's digital ledger technology. AIG and Standard Charter's reported use of the blockchain technology enabled them to create a new level of transparency in the underwriting process. Using blockchain technology, the parties converted a master policy written in the UK and three other policies written in the U.S., Singapore, and Kenya, into a smart contract that provides a shared access to policy data in real-time.

In 2014, Ethereum, invented by Vitalik Buterin, became activated. "Ethereum is a programmable, general purpose blockchain and by far the most powerful out there that can be used today." Henning Diedrich, Ethereum 27-28 (2016)(hereinafter Ethereum). Ethereum software is free and available to the public, who, by using the Ethereum platform, can create a contract that will hold a contributor's money until any given date or goal is reached. Depending on the outcome, the funds will either be released to the project owners or safely returned back to the contributors—without the involvement of a third-party financial institution or judicial officers. https://www.ethereum.org/.

A blockchain is a digital database, consisting of individual, linked records ("blocks"). As will be discussed below, each block is timestamped and tied to a previous block. Blockchain technology permits a decentralized, peer-to-peer, method of entry, but with inherent protections against changes to previously entered data. It also facilitates the use of that ledger of data to self-execute instructions and other transactions.

Over the next decade, blockchain technology has the potential to alter insurance underwriting and claims handling fundamentally. In order to decide whether this is good or bad for the insurance industry, we first have to understand what blockchain technology is not and then examine how blockchain technology originated and operates.

What Blockchain Technology Is Not

Blockchain technology is not artificial intelligence (AI), which is an area of computer science that involves machine learning of one type or another. We read about law firms starting to use AI systems like Ross or Blue Prism, but these systems are not utilizing blockchain technology. AI focuses on the ability of a software program to learn without human supervision. The software uses algorithms to extrapolate from a set of known data or parameters to discover new patterns to aid in decision making. Blockchain technology, however, can and will no doubt incorporate various AI systems into its operations.

Blockchain technology is not just peer-to-peer (P2P) computing, although it incorporates P2P in certain respects. In P2P, peers share computing resources and workload with other peers in the network. As you may recall, Napster was a publicized use of P2P, but was rooted in a central server. In contrast, P2P insurance operations are emerging that allow policyholders to initiate organizational structure, pool capital, and self-administer the insurance operation. *See* Peer-to-Peer Insurance, *available at* While blockchain technology may provide the most efficient, decentralized, and secure method for utilizing P2P insurance, its use is not the necessary condition for P2P insurance.

Blockchain technology is not the basis for the technology used in self driving cars. The creation of self-driving cars is the end result of a series of technology improvements that combine cruise control, antilock braking systems, navigation systems, and external sensors with what are called "crash optimizing algorithms," a form of AI. How blockchain technology could be integrated with self-driving cars is examined later in this analysis.

The use of blockchain technology will not just tweak how the insurance industry conducts business. If embraced, blockchain will transform it. However, all of the characteristics of blockchains briefly discussed above flow from how Bitcoin was originally created. It is to that we must now turn.

The Double-Spend Problem and the Development of Bitcoin

If I am standing next to your apple stand and I want to buy an apple from you, the transaction is pretty straightforward. I pull out a dollar bill from my wallet, I physically hand you that particular dollar and you hand me a specific apple. I cannot respend that dollar because I have physically transferred it to your possession.

Commerce on the internet, however, lacks the physical validation of our apple transaction. On the internet, digital currency needs to be transferred from buyer to seller without that same currency being spent twice. This possible use of the same digital currency for more than one internet transaction is called the "double-spend" problem. Historically, we addressed the double spend problem by relying on trusted third parties, such as PayPal or Western Union, to assure us of the validity of the electronic transaction—but always for a cost.

In October of 2008, someone (or perhaps a group of coders) calling himself Satoshi Nakamoto published a short proposal for a solution to the double spend problem: Bitcoin: A Peer-to-Peer Electronic Cash System, *available at* https://bitcoin.org (hereinafter Bitcoin). Nakamoto identified the problem as finding a way for a payee to know that the payor did not previously spend the digital currency. For Nakamoto, the only way to confirm the absence of a prior double-spend transaction was to become aware of all previous transactions involving that electronic coin. His solution was to articulate a program for a peer-to-peer electronic monetary system using a cryptocurrency labeled "bitcoin." The transformational characteristic of bitcoin is its use of a distributed ledger system—a "blockchain"—to record transactions without the use of a trusted third party.

The blockchain network timestamps transactions by hashing ("hash" is a type of mathematical and cryptographic fingerprint that will be discussed later) the transactions into an ongoing chain of what is called a hash-based "proof-of-work." This forms a record that cannot be changed without re-doing the proof of work (proof of work adds artificial computational difficulty to the ledger entry).

Nakamoto directs that you begin with the timestamp server, which operates by taking a hash of a block of items to be timestamped and widely publishing the hash. "The timestamp proves that the data must have existed, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it." Bitcoin at 2. In order to implement the distributed timestamp server, Nakamoto proposed the use of the proof-of-work system, which involves scanning for a value that when hashed, the hash begins with a number of zero bits (referring to the binary units used to represent information as ones and zeros).

> The B3i initiative is providing these companies with a platform for the efficient and cutting-edge testing and improvement of inter-company processes and to allow for the development of common standards for the insurance industry.

The proof-of-work is implemented by incorporating a "nonce" in the block until a value is found that gives the block's hash the required zero bits. (A "nonce" is a 32 bit, 4-byte, field whose value is set so that the hash of the block will contain a run of leading zeros. https://en.bitcoin.it/wiki/Nonce) "Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained in after it, the work to change the block would include redoing all the blocks after it." Bitcoin at 3. This process, as one can imagine, requires substantial computing resources and networks.

If one assumes we cannot trust anybody, then you can begin to see how proof-of-work that is hashed in helps to establish consensus and network trust. Proof-of-work becomes one-CPU-one vote. Because each copy or node of the blockchain contains every transaction, every block contains the hashed in prior proof of work, thus creating a chain of blocks that runs from the beginning transaction to the current block. As Nakamoto points out, this public history of all the relevant transactions "quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power." Bitcoin at 8.

Use of Blockchain Technology: Security, Privacy, and Smart Contracts

Don Tapscott and Alex Tapscott, in Revolution, state that rather than predicting a blockchain future, they are advocating for it, because it provides us with the best inclusive platform that can provide prosperity for the largest number of people. In their analysis, the Tapscotts identify seven functional principles of blockchain technology that demonstrate the ability to achieve these goals. Revolution 29 -51. We will focus on a few of these principles that are particularly relevant to the insurance industry.

Today, hacking, identity theft, and cybersecurity issues are the bane of internet existence. Those of us who use the internet have to rely on ever changing passwords to protect email and online accounts and we are given little opportunity to increase our security level. Nakamoto's work on bitcoin required participants to use public key infrastructure (PKI). This is an advanced cryptographic process where users get two keys that do not perform the same function: one is for encryption and one for decryption. This is accomplished through the use of hashing.

A hash function takes any input and through the use of mathematical operations produces an output of a specific size. Blockchains generally use SHA-256 algorithms (standard hash algorithm, 256-bit).

This process of applying a hash function to data is called "hashing." The result of the hash function is called the "hash." *See* Blockchain Underpinnings: Hashing, https://medium.com. In 2016, Ernst & Young provided us with a template for insurer use of PKI through hash functions for either underwriting, or the example we are going to pursue right now, claims handling.

Assume that an insured business has suffered a fire loss. There are separate property damage claims and business interruption claims. The insured wants to submit the claims information securely into the blockchain the insurer established. Some type of proof-of-work will have to be developed that can initially verify the claim information, perhaps requiring confirmation from some designated "oracle." An oracle is a conduit of information between the outside world and the blockchain. "A range of what people regard as an oracle is broad. It can be the sensor of an IoT device, but also web services that provide information in a format suitable for smart contracts to consume." Ethereum 187. Oracle services, such as Oraclize and RealityKeys, are already in existence. Ethereum 188.

First, we identify the input data that will be uploaded. This can be accounting information from the insured for the business interruption loss, video and/or photographs establishing the complete extent of the damage, plus proof of loss and other supporting documentation, all processed through a hash function. Once the hash value is obtained for each entry of the claim file, that hash value is then submitted into the blockchain infrastructure:

> INPUT DATA » HASH FUNCTION » HASH VALUE »UPLOAD.

All of the hash values are aggregated and submitted as a single aggregate hash value into the claim blockchain. The use of this type of encryption, as Ernst & Young notes, "enables the individual properties and attributes of each transaction (including claims) to be verified without reliance on trusted parties and manual intervention. There are no keys to be compromised or revoked; just mathematical proof of signing time, origin and integrity of the transaction." *See* Blockchain Technology as a Platform for Digitization, *available at* http://www.ey.com.

The blockchain used by an insurer can be public or private. The former mode is "public" in one of two forms: (1) anyone, without permission by another authority, can write data; or (2) anyone, without permission granted by another authority, can read data. Private blockchains, are as the term indicates, closed networks. A private blockchain network is composed of members who are known and trusted, *e.g.*, an industry group such as B3i. *See* Blockchain Underpinnings: Hashing, https://medium.com.

> Today, hacking, identity theft, and cyber-security issues are the bane of internet existence. Those of us who use the internet have to rely on ever changing passwords to protect email and online accounts and we are given little opportunity to increase our security level.

Another principle that the Tapscotts discuss in Revolution is privacy. The authors note that people should control their own data. Privacy is preserved by the nature of the functioning of the blockchain. The blockchain does not need to know who anybody is. In the bitcoin blockchain, the identification and verification layers are separate from the transaction layer. In other words, a bitcoin from Party A is transferred to Party B's address, but there is no reference to anyone's identity in that transaction. The blockchain network confirms that A both controlled the amount of bitcoin specified and also authorized the transaction before it recognizes A's message to transfer the bitcoin to Party B's address. The Tapscotts observed:

> On the blockchain, participants can choose to maintain a degree of personal anonymity in the sense that they needn't attach any other details to their identity or store those details in a central database. We can't underscore how huge this is. There are no honeypots of personal data on the blockchain. The blockchain protocols allow us to choose the level of privacy we are comfortable with in any given transaction or environment. It helps us to better manage our identities and our interaction with the world.

Revolution at 43.

Blockchain technology also provides a manner in which we can preserve ownership rights. Blockchains can serve as public registries for deeds, titles, or licenses. In other words, a blockchain system can provide means of proving ownership and preserving records without government oversight or control. A corollary to blockchain as a ledger of property rights is that it can also serve as the platform for the transfer, from one party to another, of such property rights. This is accomplished through self-executing agreements known as "smart contracts."

Nick Szabo provided the early analog illustration of smart contracts through the use of a vending machine. Once I drop my coin into the vending machine and push the numbers and letters that select a product in the vending machine, the transaction becomes automatic. Once the money is paid and the instructions are given, the transaction cannot be stopped and the money is not returned if the product is supplied. The transaction is self-executing.

Canadian lawyer, Josh Stark, identified two different ways of talking about smart contracts: by discussing code that is stored, verified, and executed on a blockchain (smart contract code); or alternatively, by referring to a specific application of the technology as a substitute for legal contracts (smart legal contracts). *See* Josh Stark, *Making Sense of Blockchain Smart Contracts, available at* http://www.coindesk.com.

With respect to smart contract code, Stark notes that it has unique characteristics compared to other types of software:

> First, the program itself is recorded on the blockchain, which gives it a blockchain's

characteristic permanence and censorship resistance. Second, the program can itself control blockchain assets—*i.e.*, it can store and transfer amounts of cryptocurrency. Third, the program is executed by the blockchain, meaning it will always execute as written and no one can interfere with its operation.

According to Stark, smart legal contracts are a way of using blockchain technology to compliment, or replace, existing legal contracts. Smart legal contracts would most likely be a combination of smart contract code and more traditional legal language. "Commercial agreements are full of boiler plate clauses that protect parties from various edge-case liabilities, and these are not always suitable for representation and execution through code, meaning that smart legal contracts will require (at least for the foreseeable future), a blend between code and natural language."

Smart contracts present a use case for both underwriting and claims handling. Suppose you have an insured who wants to purchase a single-person health policy and wants to negotiate the premium based on underwriting factors such as age, type of employment, lifestyle, eating habits, daily exercise, and possible medication usage. The insured fills out an application and provides the attendance data from the health club of which the insured is a member, provides the data from the Fitbit or similar device the insured wears, provides information from any healthcare app that monitors or even administers medications, and provides access to prescription medication records. All of this data is encrypted through hashing and uploaded onto the insurer's blockchain, which contains a predetermined set of categories that aggregates the information and calculates a premium based on the insured's current health, exercise, and lifestyle. This information could be fed on a continuous (at the least a monthly) basis to the blockchain that would allow for modifying the premium on a quarterly basis, according to terms set in self-executing smart contracts. If certain health parameters are uploaded, then the premium goes up or down, according to predetermined terms in the policy and according to self-executing agreements.

On the claims-handling side, smart contracts could function in certain defined situations. In particular, with the advent of the Internet of Things (IOT), and the availability of transmission of electronically stored information from interconnected devices, it becomes possible for claims handling, under certain circumstances, to be streamlined. An example of IOT use in a blockchain situation is provided by the Tapscotts in their discussion of Filament, an American company that is installing "taps" on power poles in the Australian Outback. These devices can talk directly to each other at distances of up to 10 miles. Because the power poles are approximately 200 feet apart, a motion detector on a pole that is falling will notify the next pole 200 feet away that it is in trouble. With the taps 20-year battery and Bluetooth low energy, customers can connect to the devices directly with their own phone, tablet, or computer, and the tap can contain numerous sensors to detect temperature, humidity, light, and sound. Revolution, 146–47.

> Insurers have to consider the creation of a blockchain claims-handling system. Such a system would upload, securely and indelibly, all information created in the claim process. Both insurer and policyholder would have access through PKI to the content of the claims-handling file on the public portion of the blockchain.

There is no reason why this sort of sensoring system could not be installed on farms for use by crop insurers. Combining the on-ground information along with GPS and weather station data adjacent to the farmer's fields, would allow insurers to underwrite an initial policy more quickly and efficiently and provide subsequent claims-handling services. A series of discrete "if-then" smart contracts related to specific crops could be used to facilitate claims payments if temperatures during a certain time frame fall below or rise above a certain benchmark. This type of automation would reduce the risk of subjectivity in claims handling and streamline claims payments, while reducing the possibility of fraud.

Earlier, we noted that the technology behind self-driving cars is not based on blockchain technology. Imagine, however, two self-driving cars, the purchase of which were recorded on various insurers' blockchains, and the data stream from which was recorded on those insurers' blockchains. One of these self-driving cars is involved in an accident with the other self-driving car. Using the type of smart contracts discussed above, with the complete set of timestamped, permanently recorded data on speed, direction, and location, the blockchain, through smart contracts, could adjust the claim automatically—initially as to liability, and later as to repair costs.

Blockchain and the Future of Insurance

Walter Benjamin, in his ninth Theses on the Philosophy of History, addresses a Klee painting named "Angeles Novus." This painting shows an angel looking as though he is about to move away from something he is fixedly contemplating. For Benjamin, this is how one pictures the angel of history, whose face is turned toward the past. "Where we perceive a chain of events, he sees one single catastrophe which keeps piling wreckage and hurls it in front of his feet. The angel, as angels are inclined to do, would like to stay and make whole what was is smashed, but a storm is blowing from Paradise and it entangled his

wings with such violence that the angel can no longer close them. The storm irresistibly propels him into the future to which his back is turned, while the pile of debris before him grows skyward. This storm is what we call progress." Illuminations 257–58 (1977).

Successful institutions often resemble Walter Benjamin's angel of history. Turned to the past, their view is fixed on whatever events either increased or decreased their success. They want to anchor their future plans in their past successes and to avoid their past failures. Blockchain technology provides an opportunity for the development of a future-oriented approach to marketing, underwriting, and claims handling in insurance.

Many of the bad faith claims I defend for my clients arise from allegations that the insurer failed to investigate promptly or evaluate a claim fairly. In other words, the claims are often rooted in human failures to implement institutional process. The claims are often exacerbated by lack of trust between policyholder and insurer and lack of transparency concerning the claims handling processes.

Insurers have to consider the creation of a blockchain claims-handling system. Such a system would upload, securely and indelibly, all information created in the claim process. Both insurer and policyholder would have access through PKI to the content of the claims-handling file on the public portion of the blockchain. The claims file can be generated from information already stored on the blockchain (*e.g.*, verified fire investigation reports, police reports, etc.) or from "oracles."

A claims-handling blockchain described above could also be utilized by underwriters in determining the status of the risk being insured. All of the information would be there and accessible without the need of consuming claims handlers time in coordinating the information. These could be either discrete blockchains or integrated blockchains that follow a particular insured from first application through the issuance of the last policy.

Personal lines home insurers, an area where post-loss fraud is a plague, could adapt blockchain technology to time-stamp original information about the insured, contents, the dwelling, etc., and trace through updates and changes to personal property and the dwelling itself. Such a smart, contract-based homeowners' insurance policy, as part of a blockchain, provides both insurers and policyholders with a mechanism to manage claims in a transparent fashion. If the underwriting and prior claims history is complete and was established for a sufficient period of time, it may be that the insurer and policyholder would be able to create smart contracts that would allow the policyholder to self-administer the claim if the information was already contained on the blockchain or was obtained through certified and accepted oracles. Bad faith claims should be few where the insured is part of the claims handling process.

On the reinsurer side, reinsurance may be very well suited for implementation of blockchain. A reinsurer may enter into a treaty in which it agrees to pay the ceding insurer under certain, predefined circumstances. To the extent that the underwriting of the risk in question was placed on a blockchain, it would be available to both reinsurer and ceding insurer to establish the existence and operation of the risk. Given the existence of a sufficient information base, the presumptive immutability of the information on the blockchain, and the use of trustworthy oracles, it may be that claims payments could be automated to a certain extent through the use of smart contracts. Hopefully, the work of B3i will validate this paradigm.

It is important to remember, however, that the formation of insurance contracts and the payment of claims under insurance contracts, often involve nuanced information and communication subject to various interpretation. It may be that manuscripted insurance policies used by a small number of insureds will not be amenable to transition to blockchain. This discussion is really directed at larger, form based markets.

It may very well be that, while large parts of first-party property coverages could be sold in a smart contract format, only portions of liability policies may be amenable to presentation as a smart contract. For example, as the Internet of Things expands, and smart home products become more prevalent, it will be easier to use smart contracts to connect the devices with the underlying property policy. On the liability side, however, the application of various exclusions (in particular, intent based exclusions) will not be amenable to "if-then" smart contracts. Liability policies may require some sort of synthesis between traditional policy forms and endorsements embodying smart contracts.

Additionally, it is important to note that blockchains, as we noted above, require tremendous computing power and large networks of computers. Insurers, like all large corporations, will require a substantial investment in order to create the infrastructure necessary to make the blockchain functional. Even with the continuing refinements and developments in computing power, in the near future there will be significant restrictions on the ability of insurers to engage in the type of high volume data input and storage that are required for blockchain use. The implementation of blockchain technology by the insurance industry over the next five to ten years may be uneven and inconsistent.

Conclusion

Looking to the past may not always help us to predict the future, but progress need not be an uncontrollable storm. Segments of the insurance industry are already beginning to adopt various types of blockchain systems and it will take a collective effort by the insurance industry to provide uniform frameworks and commonly accessible systems for expansion of blockchain use through smart contracts. To my lawyer friends interested in learning how to write smart contracts, I advise you to go back and relearn Basic.

In an industry regulated by 50 different states, regulatory acceptance of insurance policies that contain smart contracts will present a challenge. The insurance industry should start now to work with the National Association of Insurance Commissioners to promulgate uniform laws relating to the creation of and recognition of smart contracts for use in insurance policies. This will not happen overnight, but it is going to happen, and we should prepare for it.