NAIC National Association of Insurance Commissioners & The Center for Insurance Policy and Research
CIPR newsletter

Insurance: The Highest and Best Use Case for Blockchain Technology

*By Daniel R. Robles, PE, MBA, founder of The Ingenesist Project and chairman of the FinTech Task Force for the National Society of Professional Engineers**

**The views expressed in this article are the opinions of the author. This article is not meant to represent the official position of the NAIC or its members.*

◆ Introduction

The purpose of this article is to introduce the reader to blockchain technology and to explore how it may be used to assist with identifying and facilitating risk transfers in the insurance industry. Blockchain technology carries a promise of great opportunity and efficiency in business operations and governance. This article demonstrates how blockchain technology could be integrated broadly and uniformly across society as well as the implications for the insurance industry. Blockchain development should not be the exclusive domain of a single sector, such as banking, nor venture-funded start-ups with ultra-high return on investment (ROI) requirements. Likewise, purely decentralized autonomous organizations are not recommended because there is the risk of operating in an extralegal sector where legal recourse may not necessarily be available when things go wrong.

The primary objective of blockchain technology should be to reduce the cost of capital by the decentralization of risk. In doing so, blockchain innovation can then be applied broadly, evenly and intentionally across the economy. This makes sense because when building anything complex or important, one logical piece needs to go in front of the next logical piece regardless of its individual ROI, because the collective ROI is the true basis of valuation. If people tried to build an airplane in the same manner we are now trying to build decentralized economics, a few may benefit, but an air transportation system, as a whole, would be severely constrained.

This article suggests the place to begin developing blockchain technology is through a consortium of insurance and professional engineering entities in the creation of relevant infrastructure and its derivatives upon which everyone depends. This includes renewable energy, clean air, water, transportation systems, health and welfare, building systems, computer networks, etc. After all, bitcoins are not worth a whole lot when the power goes down.

Infrastructure projects, and all their beneficiary derivatives, require financial institutions that can bridge the gap between the inception of a project and revenue from the project. This period of time is rife with peril because the "money and title" precedes the delivery of the physical asset. The cost of capital is directly proportional to the risk associated with project delivery. Wherever the insurance industry is capable of pooling project risks, the cost of capital is greatly reduced. The insurance industry is an imperative component to this objective.

This idea represents both the challenge and the opportunity facing insurance and engineering industries related to blockchain technology. In order to arrive at these ideas, the following paper is organized into roughly 3 parts.

- Part 1 answers the question: What problem does blockchain solve? This article begins with a brief history of databases and draws the connection to how society organizes itself around technology and why organizational incentives are important to insurance.
- Part 2 suggests if each component part of the blockchain system is insurable, so too should the entire system. The insurability of the individual components of a blockchain ecosystem, revealing a somewhat mixed outcome will also be discussed.
- Part 3 identifies how the insurance industry and the professional engineering industry together can bridge the capitalization gap in blockchain system insurability.

Taken together, insurance and engineering may have a profound opportunity to create a hybrid path crossing the digital-to-physical divide for everyone to cross, including banks, venture capitalists, entrepreneurs and decentralized autonomous organizations, to far greater financial benefit than attempting to go it alone.

◆ Part One: What Problem Does Blockchain Solve?

The Block Chain Protocol is a brilliant set of ideas that cannot be uninvented. Blockchain is here to stay and will likely appear in many forms and adaptations with or without the so-called crypto-currencies that often receive the most media attention. As we enter the next phase of blockchain development and adoption, it is now recognized that bitcoin (lowercase b), as a currency, has several flaws continuing to limit its ability to completely replace money as we know it. However, Bitcoin (upper case B), as a protocol for the exchange of value, will likely remain an extremely important innovation that will continue to be adapted in many forms.

The main problem blockchain solves results from the fact computer databases simply cannot talk to each other without a layer of expensive fault-prone human administration

(Continued on page 18)

or bureaucracy. Blockchain technology is a new software architecture providing shared, immutable records—making processing transactions less error-prone. This software enables process efficiency, as well as organizational efficiency. Blockchains may apply everywhere people interface with a computer database. It is easy to envision the magnitude of this potential.

Before Bitcoin, if a person sent a contract over email, each party would hold an easily manipulated identical copy. After Bitcoin, a person can send a contract electronically, and the receiving party would hold the only valid copy. While this may sound trivial at first, it is extraordinarily difficult for a computer to perform. But to accomplish this would, in effect, allow computers to perform some, but not all, of the administrative functions administrators routinely perform today at nearly every interaction with a computer.

Not unlike mechanization of the last century, once achieved, the software-administered management will be faster, more reliable and cheaper, while the marginal cost of adding additional capacity approaches zero. Blockchain may scale up to handle large and complex transactions or scale down to accommodate billions of micro-transactions. Also like mechanization, society will certainly reorganize around these new forms of value creation and exchange. This is already evident with the extraordinary amount of venture and investment capital and creative new decentralized autonomous organizations pouring into blockchain space.

The technology required to accomplish this is complex, and until Bitcoin, it was not obvious how such a thing could be accomplished at scale. Bitcoin taught the world a great deal with its success and its limitations. However, the fact remains it is extremely difficult for a computer to make human-like decisions, and the full breadth of human capability is still well outside the reach of blockchains. Meanwhile, the potential risk-sharing partners in this technology have not yet determined the full implications, nor even created the effective vocabulary to describe its switches, knobs and pedals—let alone the blocks and chains.

Technology Reorganizes Society

The importance of blockchains includes their impact on how people may reorganize in a community. For insurance companies, the organization (mutualization) of likely perils is a core aspect to correct pricing of insurance products. To understand these implications requires a brief history lesson on database architecture.

In the early days of computer networks, machines that performed computations were connected with wires to other machines that stored data on some physical medium such as magnetic tape. Humans interacted with these machines by using finger symbols (keyboard) and changing reels of magnetic tape. These activities had very little to do with the computation actually being performed. While we may not realize it, those same functions are still often performed today in one form or another every time we interact with a computer database.

Over time, databases became so incredibly useful that companies and institutions stored all of their data in proprietary silos, where they could control access to financial records, product specifications, trade secrets, personnel files, customer data and sales projections, etc. The database for an aircraft manufacturer was structured entirely differently from a database for a coffee shop chain or an insurance company. The specialized linkages formed between the data and the operations became unique to the organization and, in many cases, proprietary. The purpose of management was to let nothing in or out of the database without permission. It has been widely written how institutions have become defined by their data structures.

The problems with legacy databases became apparent when the need arose for one database to communicate directly with another database. But this was impossible without human administration. With the advent of the Internet and social media, widespread networking capability between computers (nodes) became exponentially more valuable, while the ability for computers to communicate with each other remained linear. While electrons moved at the speed of light, many systems remained limited to the speed of bureaucracy.

In the 1990s, organizations introduced legions of administrators, intermediaries and brokers to help databases communicate with each other. More recently, database engineers invented special interfaces (APIs) that allow, say, Amazon.com to provide access to parts of their database to wholesalers or partnered retailers. APIs allowed for a wave of innovation associated with the ecommerce movement and much more. However, even APIs had significant shortcomings with more formal transactions.

For example, with all the APIs in the world, a real estate broker in 2016 must still wrestle with several databases in order to complete a transaction. They must lead the buyer and seller around the multiple listing service database

(Continued on page 19)

(MLS), as well as coordinate a lender, property inspectors, property insurance, escrow service and title insurance—all under strict government regulation and management oversight. The agents must deliver all of these databases in relative unison to a single point in time to receive signatures, a "time stamp," and become registered in public archives. And, the deal can still be reversed by a legal challenge. The process can take weeks or months, with unnerving cost frictions and price volatility.

"This is all very weird, only we've become accustomed to it." — Vinay Gupta

Unfortunately, as the value of data increases, so too are the incentives, probability and the consequences of cheating, especially where the ability to cheat has been equally enhanced by the same imperfect technologies. Additional laws and regulations are sometimes applied, which may thwart innovation to a greater degree than the protection those laws may provide. Today, asymmetric information, blanket legislation and selective enforcement are considered among the scourges of modern day commerce. Keep in mind much of this has very little to do with the actual thing that is trying to be accomplished.

What if we can get rid of all of those hindrances? What if we can eliminate the brokers and intermediaries and the bureaucracy and the administration and the noise and the friction, etc?

Actually, this is a popular idea attempted throughout history in various forms of governance and marked by the willingness and ability to control information. Obviously, there are many methods for applying control (or not applying control); most lay on a spectrum between a fully centralized organization and a fully decentralized organization. The benefits and drawback of each are well understood from historic references—that is, until blockchain technology arrived.

Centralization

The first way to enable databases to communicate with each other is to consolidate and combine them into a single database hoping enough commonality would exist to patch them both together. These are aptly called "acquisitions and mergers" where two somewhat similar entities combine their data under a central authority. Efficiencies are gained in scale and elimination of redundancy. Unfortunately, centralization can also lead to inefficiencies such as top-heavy hierarchy, monopoly, obfuscation, stagnation and vulnerability to groupthink or external shocks. Failures would often trigger blanket legislation. Meanwhile, the original problem remains: How do these new mega databases communicate with other mega databases?

Decentralization

The other way to eliminate intermediaries is for everyone to share the same database between organizations. Multiple writers can retrieve and populate data simultaneously with no controls, consensus or centralized authority. Natural organic linkages would form and operations would become faster, cheaper and easier to perform and maintain. The network effect can take hold where the value of the network would grow exponentially. Unfortunately, there would be no way to stop a person from cheating another person, or going back to change the conditions of a contract, or giving himself a raise or double spending a unit of account, etc. For decentralized databases, these are precisely the problems blockchain solves.

What Does This Mean for Insurers?

People and organizations will reorganize around this new type of data and value exchange system much like they earlier reorganized around prior technologies, such as typing pools. This represents a new set of business perils that do not necessarily pool well with the old set of business perils upon which current insurance products are based. In essence, the insurer is faced with four primary concerns.

- How different would it be to insure a decentralized business or business processes than a centralized set? What historic data are still valid? What data needs to be collected anew? How much can the insurer rely upon a management system comprised of nothing but software? How does an insurer assert dominion over economic value denominated in cryptographic tokens that are neither money nor property according to the law? Who do you call when things go boom?
- The insurance industry itself is an administration-laden database. Could it operate on a blockchain? What are the opportunities and implications of culling their own legions of brokers and staff? Would an insurer be willing to insure a company that had just culled their own brokers and staff? If they do not do it and a competitor does, what perils are then imposed on the firm? How does the insurer preserve institutional knowledge in the wake of replacing brokers with software?
- The purpose of regulation of any kind should be to encourage or discourage specific types of human behaviors. If the human is taken out of the equation, what regulations are still needed? Are there any regulations

(Continued on page 20)

standing in the way? Are new regulations required? Can regulations be bypassed or shifted to another segment of a process? How fast can regulators respond to an unanticipated condition?

- Finally, everything about database management has very little to do with the thing actually being computed. Blockchain and crypto-currencies exist in a digital realm. Meanwhile, real people are doing real things in real life where real things behave according to physical laws. How exactly will blockchain software reconcile or interact with the real world?

These are extremely important questions yet to be resolved. It is worth the time and effort to learn and understand the implications of blockchain technology because the opportunities for adoption by the insurance industry are quite literally exponential:

- Insurers may achieve efficiency with internal processes.
- Insurers may achieve efficiency insuring blockchain clients.
- Insurers may discover new markets previously unviable.
- Insurers may reduce the granularity of insurance product to tighter pools.
- Insurers may scale up or scale down (micro-insurance) at near zero marginal cost.

The insurer needs to know exactly what is being insured, the numerical probability the peril will or will not manifest, and the consequences of a failure or breakdown in the process. Problems may arise where an organization loses important institutional knowledge, adaptability and innovation due to the wholesale elimination of important administrative personnel.

The second part of this article will dissect a blockchain process into five constituent parts and analyze the insurability of each subsection. If all segments of a business process are insurable, then the entire process ought to be insurable. This second part will demonstrate how existing institutions may help bridge insurability gaps in blockchain implementations.

◆ PART TWO: THE MECHANICS OF BLOCKCHAINS

Our theory is if each component part is insurable then the entire ecosystem should be insurable. Using a simple insurability test, we can identify shortcomings of a business plan needing to be shored up with non-blockchain institutions, or we know the plan is unviable. Further, blockchain applications that are the most durable from an insurability standpoint, may also signal the best returns on blockchain investment and enjoy lower cost of capital for funding innovation.

The Insurability of Blockchains

Investment in any innovation or asset requires institutions willing to carry the cost and risk of design, development and construction of a project before—sometimes years before—the asset produces revenue sufficient to return the investment capital. The cost of capital is often the primary driver determining what can and what cannot be built. Where an investment can be insured, the cost of capital drops precipitously.

Blockchain technology is like a three-trick pony. It essentially combines three slightly clumsy computer tricks in order to mimic decisions a human administrator routinely makes with apparent ease. The difference is, if done correctly, the computer can perform some of these decisions with great speed, accuracy and scalability. If done incorrectly, the computer can also propagate an incorrect outcome with stunning efficiency.

The technique we will use to analyze insurability harks back to any "Insurance 101" textbook with the three conditions of insurability expressed as follows:

- Can we identify the risk exposure?
- What is the (mathematical) probability such risk exposure will manifest?
- If so, what are the consequences (cost) of failure?

The rules of our test are simple: All three conditions must be known in order to create an insurance product. The inability to answer any one of these questions results in a non-insurable condition. Non-insurable business methods using blockchain technology must then be augmented or rejected.

#1: The Byzantine General's Dilemma

This scenario was first described in 1982 at SRI International. This problem simulation refers to a hypothetical group of military generals, each commanding a portion of the Byzantine army, who has encircled a city they intend to conquer. In formulating their plan, it is determined there are only two ways to win the war: 1) they all must attack together or 2) they all must retreat together. Any other combination would result in complete annihilation. Obviously each general has a vested stake in the outcome of the group's consensus.

The problem is complicated by two conditions: 1) there may be one or more traitors among the leadership working for

(Continued on page 21)

the other side; and 2) the messengers carrying the votes are subject to being intercepted. For instance, if a traitorous general could send a tie-breaking vote in favor of attack to those who support the attack and a different vote to those who support a retreat, a rout could be intentionally and easily created.

A Byzantine fault-tolerant system may be achieved with a simple test for unanimity. After the vote is called, each general then "votes on the vote," verifying that his own vote was registered correctly. The second vote must be 100% unanimous. Any other outcome would trigger a default order to retreat.

Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n2) — Wikipedia.

Metcalfe's law provides a means of predicting the security of such a network would also be proportional to the square of the number of members in the network.

Insurability Test #1
Next, we apply the three conditions of insurability to the above scenario:

- Yes, we can identify the risk exposure to the generals and their armies.
- Yes, citing Metcalfe's law for networks, the probability of corrupting the network may be readily calculated using real numbers.
- Indeed, the consequences of failure would be tragic, but at least an insurance product could be offered to the families.

Therefore, #1 is insurable.

Modern Examples of Byzantine Fault Tolerant Systems
The analogy for networks is that computers are the generals, and the instruction "packet" is the messenger. To secure the general is to secure the system. Similar strategies are commonplace in engineering applications, from aircraft to robotics or any autonomous vehicle where environmental inputs are converted to movements of, say, a flight control surface. The Boeing 777 and Boeing 787 use Byzantine proof algorithms, and each are clearly insurable mechanisms in a highly regulated industry of commercial aviation.

#2: Multikey Cryptography
The Byzantine fault-tolerant strategy is useful for securing the nodes in a network (the generals). Multikey cryptography is for securing the packets of information they exchange between them. On a decentralized ledger, it is important that the people who are authorized to access information and the people who are authorized to send the information are secured. It is also important the information cannot be tampered with in transit. Society now expends a great deal of energy in bureaucratic systems performing these essential functions to prevent theft, fraud, spoofing and malicious attacks. Trick #2 allows this to be done with software.

Assume for a moment that a cryptographic key is like any typical key for opening locks. The computer can fabricate sets of keys that recognize each other. Each party to the transaction has a public key and a private key. The public key may be widely distributed because it is indiscernible by anyone without the related private key.

Suppose Alice has a secret to share with Bob. She can put the secret in a little digital vault and seal it using her private key + Bob's public key. She then sends the package to Bob over email. Bob can open the packet with his private key + Alice's public key. This assures the sender and receiver are both authorized and the package is secured during transit.

Insurability Test #2
Applying the three conditions of insurability :

- Yes, we can see the risk exposure to an unsecured message.
- Yes, we can calculate the probability of failure by examining the strength of the encryption.
- Indeed, the consequences of failure could be estimated because the contract would likely represent value.

Therefore, #2 is also insurable. Things are looking up.

#3: The Time Keeper
Einstein once said that the only reason for time is so everything does not happen at once. There are several ways to establish order in a set of data. The first is for everyone to synchronize their clocks relative to a small borough of London and embed each and every package with dates of creation, access, revision and date of exchange, etc. Then we must try to manage these individual positions, revisions and copies moving through digital space and time.

The other way to accomplish this is to create this moving background (like they do in the old TV cartoons) and indelibly attach the contracts as the background passes by. In order to corrupt one package, you would need to hijack the whole

(Continued on page 22)

train. The theory is that it would be prohibitively expensive, far in excess of the value of the single packet, to do so.

Computer software of the blockchain performs the following routine in order to accomplish the effective equivalent process: Consider for a moment a long line of bank vaults. Inside each vault is the key or combination to the vault immediately to the right. There are only two rules: 1) each key can only be used once; and 2) no two vaults can be open at the same time. Acting this out physically, it is a bit of a chore, but security is assured, and there is no way to go backwards to corrupt the earlier frames. The only question now is: Who is going to perform this chore for the benefit of everyone else and why?

Finally, Here is Why the Coin is Valuable

There are several ways to push this train along. Bitcoin uses something called a proof-of-work algorithm. Instead of hiding the combinations inside each vault, a bunch of computers in a worldwide network all compete to guess the combination to the lock by solving a puzzle that is difficult to crack but easy to verify. It is like guessing the combination to a high school locker. It is hard to do, but once accomplished, everyone can easily see the open locker; that is sufficient proof the work has been done.

Whoever solves the puzzle is awarded electronic tokens called bitcoin (with a lower case b). This is sort of like those little blue tickets that kids get at the arcade and can be exchanged for fun prizes on the way out. These bitcoins simply act as an incentive for people to run computers solving puzzles to keep the train rolling.

Bitcoin (All Crypto Currencies) Must Have Value Because If They Did Not, Their Respective Blockchain Would Stop Cold

A stalled blockchain would be the crypto-currency equivalent of bankruptcy. This may account for a fair amount of hype around the value of bitcoins. Not surprisingly, as the price increases, the better the blockchain operates.

Insurability #3

While all of this seems a bit confusing, keep in mind that we are describing the thought patterns of a computer, not necessarily a human. The important thing is that we can analyze the mathematics:

- Yes, we can see the risk exposures associated with vaults, trains and puzzles.
- Yes, we can calculate the probability that the system can be corrupted by the relative value of the coins.
- Indeed, the consequences of failure could be dire, but the hazards are foreseeable.

The Blockchain Ecosystem

So there we have it. All three are insurable and, therefore, we can say with rational confidence blockchains are insurable for their intended outcome. The problem is blockchains cannot exist in digital isolation; their value must be derived from the value of something else—something real.

Are Cryptocurrencies Actually Money?

There are many prominent articles by many smart people discussing this topic. However, at the time of this writing, according to Uniform Commercial Code, article 9, a very explicit definition for money is provided as follows:

"Money" means a medium of exchange currently authorized or adopted by a domestic or foreign government.

In terms of our insurability test, the answer is simple: No, digital tokens are not money. While their destruction may represent an economic loss, the loss would need to be denominated in dollars. The courts and enforcement cannot be invoked to protect your bitcoin. While we may be able to identify the peril and even calculate the probability of loss, we cannot predetermine the consequence of the loss and, therefore, cannot price the risk correctly.

Are Cryptocurrencies Considered Property?

There is some ambiguity here as well. When we think of property, we think of discreet units that are largely inseparable. The title to the asset travels with the whole asset as it changes hands. A lien on the property would be needed in order to assert dominion on the asset. But bitcoins are quite easily divisible, almost fluid, lubricating a blockchain. If I loaned you a car but kept the wheels as collateral, the utility of the car would be encumbered. Or it would be like holding a lien against the money to purchase the car—and not the car.

The answer for all practical purposes is that cryptocurrencies cannot really be treated as property, at least within the boundaries of law. Therefore, they are uninsurable.

Let Us Take a Look at Where We Are

	Insurable
#1 Fault Tolerant	✓
#2 Multikey Cryptography	✓
#3 Decentralized Ledger	✓
Represents Money	X
Represents Property	X

(Continued on page 23)

So, if bitcoins are not money and bitcoins are not property, what are they? How does one prove ownership? How does the owner assert dominion? How would liability be assigned for economic losses of another person in a transaction where all agreements are in the form of nonrevocable contracts executed by software? Where do rights and responsibilities attach? This is a deeply troublesome discussion if you are in the business of assuring or insuring blockchain-based enterprises.

More troubling is that these precise characteristics are what make cryptocurrencies attractive for illegal activity, thereby increasing variance of expectations rather than reducing variance—the exact counter-effect of insurance. If assets can be converted to cryptocurrency, they become difficult to seize or repossess. The extra-legal sector is categorically uninsurable by mainstream carriers.

The insurance industry is faced with both a dilemma and an opportunity to build specialized insurance for blockchains, or bridge the insurability gap with mainstream markets, or both.

Clever legal scholars have suggested perhaps ownership may be established with a claim against the cryptographic keys that open and close the packets. This is a very interesting idea. We have already established that these nodes and these keys are insurable. Logic may be built into key distribution to assign liability or limit liability and, thus, price risk correctly.

◆ PART THREE: BRIDGING THE CAPITALIZATION GAP

In Part 1 we identified the problems blockchain solves. In Part 2, we identified the problems blockchains cannot solve. In this part, we will try to specify a bridge one might build across the chasm upon which everyone from banks, entrepreneurs and modern decentralized organizations may cross.

One alternate approach rarely considered is a hybrid model of physical proofs interchangeable with the digital proofs in a blockchain, as needed or where appropriate.

For example:

- Instead of computer modeling a fake network of Byzantine generals, a network of real generals can be set up to model a computer network.
- Instead of a solution to a trivial puzzle as a means of generating a digital token, the solution to a real life puzzle can also be used to generate a digital token.
- Instead of a hashing program generating a cryptographic key, a person's resume could be used as the algorithm to hash cryptographic keys authorized to open and close packets on the blockchain.
- Etc.

As long as each component of the blockchain ecosystem is insurable, the entire system would remain insurable. There would otherwise be no limit to the number of blockchains that can exist nor the number or combination of analog and digital components that can be mixed as long as the tokens, in the end, can clear accounts.

The Institution of Professional Engineering

For 80 years, the professional engineers (PEs) have been trusted third-party adjudicators for banks and insurance companies. The prevailing purpose of PEs is to safeguard the health and welfare of people and property—and by extension, the insurers and banks and assure them. Professional engineering allows people and projects to span the capitalization gap—that is, the time gap between the initiation of investment and the delivery of revenue from the investment. The professional engineering process, in fact, provides many of the same security functions as the three tricks of Blockchain technology.

- PEs endure a peer review process in obtaining and maintaining their license. Examinations qualify the engineers and a revocable license established an incentive to high integrity. This bears similarity to the Byzantine general's network.
- PEs use a common science and language of mathematics as the public key and their respective problem solution as the private key effectively encoding their judgments. An engineer recognizes the information of another engineer and can validate the integrity of a packet of information. This simulates multikey cryptography.
- The PE's stamp acts to finalize a transaction to an indelible legal ledger memorializing monetary value and title to property.

The continued similarities between the goals of blockchain protocol and the professional engineering protocol are remarkable—thus, demonstrating individually, blockchain ideas are not new and may in fact be more compatible to existing institutions than previously considered. Perhaps an effective blockchain can be constructed combining components of each realm, real and virtual, to achieve high ambi-

(Continued on page 24)

COMPARISON AND SIMILARITIES BETWEEN BLOCKCHAIN PROTOCOL AND THE PE PROTOCOL

Attribute	*Blockchain Protocol*	*PE Protocol*
Fault Tolerant	Yes	Yes
Objectivity	Programmed rules and computer algorithm	Engineering laws and principles.
Governance	Trusted third party to administer databases.	Trusted third-party institution to the public, banking and financial institutions for 80 years
Permanence	Transactions are executed by programmed set of rules that are indelible.	Works of engineering, by nature, are irreversible and indelible by observation.
Consensus	Computers that vote on the vote reach consensus. Mining puzzle is difficult to solve but easy to prove.	The professional engineer stamp secures the nodes by peer review. Engineering puzzles difficult to solve but easy to prove.
Chronology	A string of indelible blocks establish chronological order of contracts in time.	Professional engineering stamp and permitting establish chronological order of physical state
Security	Security is provided with cryptography that is very difficult to guess but very easy to prove.	Security is provided by licensure, which is very difficult to obtain/fake but very easy to prove.
Transparency	A blockchain can be audited to track cheaters or validate transactions.	Engineering is naturally auditable. Processes track risk exposures.

guity (human capability) while also providing speed, accuracy and scale (computer capability). The National Society of Professional Engineers (NSPE) and the NAIC are at an important point in history. They can either wait to see if this new technology will render important institutions irrelevant, or they can use this technology to amplify the current roles as a "financial institution" in their own right.

The Insurability of Engineering

During the design and construction phase of a project, the asset lives on a balance sheet only as an engineering design. The engineering stamp serves as proxy for the future title and revenue of the project. Insurability is contingent on engineering sign-off. If a project were not insurable, then a bank would not lend money to it.

This scenario is routine and commonplace in modern finance given the insurability of professional engineering and its ability to bridge the capitalization gap. Let us now take a look at where we stand on blockchain system insurability:

Insurability Matrix	Blockchain Ecosystem	With Professional Engineering
#1 Fault Tolerant	✓	✓
#2 Multikey Cryptography	✓	✓
#3 Decentralized Ledger	✓	✓
Represent Money	X	✓
Represent Property	X	✓

Oracle Contracts

A "smart contract" is a decision executed by a computer algorithm on a blockchain. For example, if condition A and condition B are triggered, then payment C is executed. An

(Continued on page 25)

adjudicated smart contract is a smart contract whose execution is contingent on a physical observation or judgment by a reliable witness.

An Oracle contract is an adjudicated contract with the added requirement the adjudicator is deemed the most appropriate person to be performing the adjudication. These additional requirements mean a method is required to establish the most appropriate adjudicator, and the method must likewise be insurable. The Oracle must make decisions in physical space—not simply assess digital data. The Oracle must be able to be present in time and space, determine causation of an event and deal with significant ambiguity in relation to the facts being observed. The validity of the Oracle is what establishes tangibility and invokes law—therefore, money and property. Securing the pool of decentralized Oracles would be essential to insurability of such contracts on a blockchain.

Banks and insurance companies depend on engineers to verify the design, materials, processes, components and performance of all subjects they finance. In general, the construction process breaks down into a long and complicated series of events that all must be contracted, negotiated, ordered in time and verified in a secure manner while also triggering payments to stakeholders. These events are tied together by critical path methodology. All actuarial data used to insure any number of insurable conditions at some point touches the professional engineering stamp. A structure cannot be occupied without the PE stamp; a car cannot be insured without safe roads and bridges; a municipal project cannot be capitalized without licensed engineers assessment, etc.

Likewise, subsequent innovation such as autonomous motor vehicles; Internet start-ups and blockchain enterprises are collectively contingent on safe roads, reliable computer networks and renewable energy, and are thus contingent on insurable Oracles. Professional engineering is the best model to start with because it is already codified and insurable. It will be essential to broaden the breadth and depth of the Oracle pool as blockchain implementation advances. However, the insurability requirements must remain in order for the global blockchain experiment to be ultimately successful.

The promise of Oracle contracts is that the Oracle pool may itself be decentralized and distributed broadly across society to include a strong diversity of domain experts. As long as this process is insurable, there are no limits to who and how many Oracles may act in a network.

The Oracle would essentially flip the switch allowing the computer to follow a path of logic to, say, approve the next step in a sequence of events; assign, limit and transfer liability; shift insurance coverage; establish responsible charge; or initiate a payment from a bank, bond, insurance claim or contingency fund. If there is a problem or suspected corruption, the entire trail can be audited and unwound to forensic standards.

◆ CONCLUSION

We may have been here before. Many of the issues brought up in this article were also present during the time of this author's participation in the North American Free Trade Agreement (NAFTA) negotiations. Anyone who was around in the early 1990s may remember the mantra of modern globalization was that decentralized markets were good and centralized markets were bad. The mathematics supporting the efficiencies of the comparative advantage economic model was, and still is, indisputable. Unfortunately, decentralized markets were administered unevenly, disproportionately and were only partially insurable, at best. The act of trying to control a decentralized market eliminated many of the benefits of having one. Today, we may face a similar peril, except with a far more powerful technology promising exponential efficiencies or exponential deficiencies. The difference is that we also have the knowledge, foresight and the profound responsibility to get it right this time.

The consortia between engineering and insurance already exist, and their impact on the cost of capital is abundantly clear. To formalize this on a blockchain initiative is not a radical position by any means. What is unique about this proposal is that insurance and engineering should be at the forefront of blockchain development, building the bridge spaning the capitalization gap upon which everyone else can travel.

The current path of blockchain deployment dominated by banks, venture capitalists and decentralized autonomous organizations is not sufficient in delivering the highest and best use for this important technology within the existing framework. The market incentive and corresponding regulatory overreach in attempting to control blockchains will only have the effect of re-centralizing databases rather than decentralizing databases. The further detriment of regulatory arbitrage may serve only to increase volatility and not decrease it.

The superior method for so-called "controlling" blockchain technology would be through hybrid application of digital

(Continued on page 26)

and physical proofing mechanisms that are individually insurable so that their infinite combinations would still result in easily insurable enterprise. Reinsurance could then be an umbrella. Unique combinations of such components assigned by entrepreneurs would yield the new business methods of the future at a very low cost of capital.

The Oracle pools may be decentralized through algorithms converting resumes to cryptography in a manner that secures asset nodes (titles). Real world problems can be used as proof-of-work for the puzzles that move blockchains and create their associated currency. Cryptocurrencies would no longer be just digital tokens best suited for speculation. Rather, they could represent real human productivity achieving generalized reciprocity in real money exchanges.

In the manner specified herein, blockchain technology can meet its highest potential in delivering improved financial methods to an increasingly crowded planet.

ABOUT THE AUTHOR

Daniel R. Robles, PE, MBA is the founder of The Ingenesist Project (TIP), whose objective is to research, develop and publish applications of blockchain technology related to the technical and financial services industries. Mr. Robles currently serves as the chairman of the FinTech Task Force for the National Society of Professional Engineers (NSPE), as well as a research fellow at the International P2P Foundation related to blockchain implementations.

Mr. Robles is known worldwide as blogger for www.Ingenesist.com, www.Insurancethoughtleadership.com, www.Coengineers.com and several others. He holds professional engineering (PE) licenses in Washington and California, as well as a master's degree in international business from Seattle University.

National Association of Insurance Commissioners
& The Center for Insurance Policy and Research

NAIC Central Office
Center for Insurance Policy and Research
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197
Phone: 816-842-3600
Fax: 816-783-8175

http://www.naic.org http://cipr.naic.org

To subscribe to the CIPR mailing list, please email CIPRNEWS@NAIC.org or SHALL@NAIC.ORG

The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.

The views expressed in this publication do not necessarily represent the views of NAIC, its officers or members. All information contained in this document is obtained from sources believed by the NAIC to be accurate and reliable. Because of the possibility of human or mechanical error as well as other factors, however, such information is provided "as is" without warranty of any kind. **NO WARRANTY IS MADE, EXPRESS OR IMPLIED, AS TO THE ACCURACY, TIMELINESS, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OF ANY OPINION OR INFORMATION GIVEN OR MADE IN THIS PUBLICATION.**

This publication is provided solely to subscribers and then solely in connection with and in furtherance of the regulatory purposes and objectives of the NAIC and state insurance regulation. Data or information discussed or shown may be confidential and or proprietary. Further distribution of this publication by the recipient to anyone is strictly prohibited. Anyone desiring to become a subscriber should contact the Center for Insurance Policy and Research Department directly.