Contents

Introductory note of the National Society of Professional Engineers: This whitepaper was prepared by the NSPE Financial Technologies Task Force whose members served from July 2015 to July 2016. The whitepaper was requested as a deliverable from the task force as it investigated the involvement of professional engineers in the blockchain technologies. This whitepaper is intended to explore those opportunities and how the Professional Engineering Protocol, the basis for the licensure system in the United States, and blockchain technology may intersect. Blockchain technology, though highly technical in construct, may provide opportunities for the practice of professional engineering into the next 100 years of the profession and beyond.

Executive Summary

Quite a few voices are calling the emerging blockchain technology the greatest revolution since the advent of the Internet[1], with far reaching application in banking, insurance, and government. It is recognized that any technology impacting these sectors will inevitably impact professional engineering. It is important to understand the practical opportunities, implications, and perils of what amounts to the reliance on software to execute administrative decisions.

Today, institutions interact with each other as a collection of proprietary databases that can communicate only with some form of human interface or bureaucracy. Blockchains (the technology behind bitcoin and other digital currencies) would permit multiple parties to share a single database with no central authority where access and controls are managed with software. Blockchains are very difficult to tamper with once information is registered. Any number of use cases in accounting, economics, finance, insurance, contracting, and intellectual property can be imagined.

The result would be high efficiency, great speeds, low marginal cost, and infinite scalability. Unfortunately, digital currencies—the lubrication of such databases—are struggling to achieve monetary liquidity due to a lack of intrinsic value. They exist in an extralegal domain where it is difficult to treat them directly as money or property. More importantly, digital currencies seem unable to bridge the "capitalization gap" unless marketed as an object of speculation. Despite the media attention, blockchain technology is struggling for an interface with the physical world.

By contrast, the US system for licensure of professional engineers (Professional Engineering Protocol) with its own model law, is effective in bridging the capitalization gap—i.e., that long period of time between money flowing to a product or structure and the time that project produces revenue. Within this capitalization gap, the engineer's stamp holds the asset in suspension during the design and construction phases, serving as a proxy for the finished project on the accounting balance sheet. Upon closer comparison, there appears to be significant functional similarities between the mechanics of the Professional Engineering Protocol and the mechanics of Blockchain Protocol for achieving security, consensus among stakeholders, and validation of transactions. Professional engineering licensure has proven effective for over 100 years, but few people are aware of the role that PEs play in an economic system. Today, the institution of professional engineering is struggling for an interface with the digital world.

The argument set forth in this whitepaper is that by integrating Blockchain Protocol with the Professional Engineering Protocol, several mutual needs may be fulfilled. This position is supported by using a risk analysis model rather than a more common return-on-investment (ROI) analysis. There are simply too many unknowns for an ROI model to be meaningful beyond conjecture. As such, we are able to conclude that the elimination of risk may lower the cost of capital to the extent that projects upon which society most depends will be prioritized correctly and executed appropriately using blockchain technology in a modern economy.

It is recommended that professional engineering societies form a consortium with the insurance industry to develop a decentralized human interface to blockchain contracts wherever the transfer of risk between the digital and the physical world is important. This would favor blockchain technology applied to the capitalization of public and private infrastructure upon which everyone depends. Finally, a digital currency backed by professional engineering proof of work would have intrinsic properties and adequately serve as an effective store of the value, unit of account, and medium of exchange.

Introduction

Professional engineering in the United States has existed for over 100 years. The task force posits that the professional engineer has been the trusted third party to banks, insurance corporations, and governments for providing technical design, validation, and management of large-scale projects that support public safety, welfare, and productivity. In fact, the key assumption of the task force is that professional engineering, along with banking and insurance institutions, form the three-legged stool that supports a modern developed economy. As the banking and insurance industries change, so too must the professional engineer.

With the advent of blockchain technologies—the underlying technology of the bitcoin cryptographic currency phenomenon—computer software is now capable of executing many types of financial transactions with unprecedented speed, accuracy, and efficiency.[2] Because the Professional Engineering Protocol forms the basis of national infrastructure, anything that may impact the national finance or insurance institutions can potentially involve the engineering industry and, thus, public welfare. This creates challenges as well as opportunities for professional engineering.

The four goals of this whitepaper

The task force set out to address four goals through this whitepaper. The first goal is to impress upon professional engineers that there are important functional similarities between the Professional Engineering Protocol and the Blockchain Protocol. The integration of these two protocols might have a profound and positive impact on professional engineering and therefore society as a whole, while the divergence of these two protocols could have a detrimental effect. Doing nothing would also be a suboptimal position[3].

The second goal of this paper is to notify the blockchain development community (computer engineers), investors, and entrepreneurs that building applications for the professional engineering domain may resolve many of the problems that currently constrain the blockchain industry.

The third goal of this whitepaper is to suggest to the banking and insurance industries that professional engineering integration may be the missing financial institution that can resolve many practical problems for existing industries that are now attempting to adopt blockchain technology internally.

Finally, this paper further recommends that the development of blockchain applications specifically integrating the practice of professional engineering ought to coincide or emerge concurrently with the blockchain applications under development for the financial industries.

To arrive at these conclusions, this paper is organized into three stand-alone parts:
Part 1 answers the question, what problem does blockchain solve? We begin with a brief history of databases and draw the connection to how society organizes itself around technology and why organizational incentives are important to risk management.

Part 2 develops the risk management position further to suggests that if each component part of the blockchain system is insurable, so too should the entire system and therefore, risks are manageable. Here we look at the insurability of the individual components of a blockchain ecosystem, revealing a somewhat mixed outcome.

Part 3 identifies how the insurance industry and professional engineers may collaborate to bridge the capitalization gap in blockchain system insurability.

This paper concludes that the highest and best use for blockchain technology is to reduce the cost of capital by decentralizing risk, not necessarily money—yet. This position is somewhat contrary to current trends to "build a better currency."

Instead, we propose a means of mitigating project risks by combining professional engineering with blockchain technology to solve real problems that threaten our economy and infrastructure, as well as accelerate technical innovation, and therefore underwrite a better currency.

Part 1: What Problem Does Blockchain Solve?

The main problem that blockchain solves results from the fact that computer databases simply cannot talk to each other without a layer of expensive fault-prone human administration or bureaucracy. Blockchain technology is a new software architecture that provides shared, immutable records that make processing transactions far less error prone and far more efficient. This software enables both process efficiency, as well as organizational efficiency. The applicability of blockchains may include every situation in which people interface with a computer database. It is easy to envision the magnitude of that potential.

Absent the Blockchain Protocol, if a person sends a contract over e-mail, each party would hold an identical copy that could be easily manipulated. Using the Blockchain Protocol, a person can send a contract electronically and only the receiving party would hold a valid copy. While this may be as simple as a handshake for people, 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 routinely performed today by humans at nearly every interaction with a computer database.

Not unlike autonomous vehicles of the future, once achieved, the software-administered autonomous management will be faster, more reliable, and cheaper, while the marginal cost of adding additional capacity will approach zero. Blockchain may scale up to handle large and complex transactions or scale down to accommodate billions of microtransactions with little overhead. Much like mechanization in the past century, 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 organization (DAOs) pouring into the blockchain space[4].

Technology Reorganizes Society[5]

Over the last 50 years, computer 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 specs, trade secrets, personnel files, customer data, sales projections, etc. The database for an aircraft manufacturer, for example, is structured entirely differently than a university, or an insurance company. The specialized links that form between the data and their corresponding human operations become unique to the organization and in many cases, proprietary. The purpose of management is to let nothing in or out of the database without permission. It has been widely written how institutions have become defined, or “reified” by their data structures.

The problems with legacy databases became apparent when the need arose for one database to communicate directly with another database. Unfortunately 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 flat. Electrons moved at the speed of light, but many business 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, called application program interfaces (API), 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 e-commerce movement and much more. However, even APIs have significant shortcomings with more formal and complex 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 an otherwise simple transaction. They must lead buyers and sellers around the multiple listing service database (MLS), coordinate with lenders, property inspectors, property insurers, escrow services, and title insurers, 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. Buyers and sellers are not allowed to interact with each other directly, and the deal can always be reversed by a legal challenge, even after closing. The process can take weeks or months with unnerving cost frictions, price volatility, and opportunity costs. None of this has anything to do with what should really be a very simple transaction. This is extremely inefficient, but we've become accustomed to it.

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 often applied, which may thwart innovation to a greater degree than the protection that those laws may provide. Today, asymmetric information, blanket legislation, and selective enforcement are considered among the scourges of modern-day commerce. *Keep in mind that 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 that? What if we can eliminate the brokers and intermediaries and the bureaucracy and the administration and the noise and the friction?

Actually, this is a popular idea that has been attempted throughout history in various forms of governance models 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[6]

The first way to enable databases to communicate with each other directly is to consolidate and combine them into a single database, hoping that enough commonality would exist to patch them 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 external shocks. Failures would often trigger blanket legislation. Meanwhile, the original problem remains unsolved: How do these new megadatabases now communicate with other megadatabases?

Decentralization[7]

The other way to eliminate intermediaries is for everyone to share the same database between many organizations. Multiple writers can retrieve and populate data simultaneously with no controls, consensus, or centralized authority. Natural organic links 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, going back to change the conditions of a contract, giving himself a raise, or double spending a unit of account, etc. *For decentralized databases, these are precisely the problems that blockchain solves.*

High-Level Implications[8]

People and organizations may soon reorganize around this new type of data architecture and value-exchange system much like they earlier reorganized around prior technologies. Many new questions arise:

1. How different would it be to insure/assure a decentralized business or business processes than a centralized set of processes? Who holds liability when things go wrong?
2. The corporations in question are themselves often large and complex administration-laden databases. Could they operate on a blockchain?
3. The purpose of regulation of any kind is to encourage or discourage specific types of human behaviors. If the human is taken out of the equation, what regulations are still needed?
4. Blockchain and cryptocurrencies exist in a digital realm. Meanwhile, real people are doing real things in real life. How exactly will blockchain software reconcile or interact with the physical world?

Risk Management 101

You can't make a bet without odds. Banks, insurers, and engineers must answer these same three conditions in order to manage and price risk correctly:

1. What exactly is the peril being assured?
2. What exactly is the numerical probability that the peril will manifest?
3. What exactly are the consequences of a failure?

In the following section, we will dissect a blockchain business system 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.

Part 2: The Mechanics of Blockchains: A Three-Trick Pony

Today, billions of dollars of venture capital, corporate investment, and swarms of start-ups are working feverishly to design and deploy new business methods (and reboot old ones) that incorporate blockchain technology[9]. 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. Project risk is the primary driver of the cost of capital. The cost of capital is often the primary driver determining what can and what cannot be built and in what order or priority, i.e., money defines the critical path.

Where an investment can be insured, the cost of capital drops precipitously. Clearly, the applicability of risk management principles is important. Our theory is that if each component part is insurable then the entire ecosystem should be insurable. Using the simple insurability test from Risk Management 101 above, we can identify shortcomings of a blockchain business plan. This allows us to quickly adopt or reject a business plan. Moreover, blockchain applications that are the most insurable may also signal to the market the best returns on investment, thus enjoying lower cost and higher returns on investment.

Definition: Blockchains are a ***technology for shared databases between multiple non-trusting writers, yet can be modified and authenticated without a trusted intermediary***[10]*.*

The Insurability of Blockchains

Blockchain technology is like a three-trick pony. It essentially combines three slightly clumsy computer procedures in order to emulate decisions that a human administrator routinely makes with apparent ease. The difference is that, if done correctly, the computer can perform some of these decisions with incorruptible speed, accuracy, and scalability. However, if done incorrectly, the computer can also propagate an unintended outcome with the same staggering efficiency.

Restated, the technique that we'll use to analyze insurability harkens back to any "Insurance 101" textbook with the three conditions of insurability expressed as follows:

1. Can we identify the risk exposure?
2. What is the [mathematical] probability that such risk exposure will manifest?
3. If failure occurs, what are the consequences [cost] of that failure?

The rules of our test are simple: All three conditions must be known in order to create an insurance product or any mitigation strategy. The inability to answer any one of these questions results in a noninsurable condition. Any noninsurable business methods must then be corrected or rejected. Likewise, any noninsurable blockchain business proposition would, by definition, be irrational, dependent on media hype, or suspect for speculation—and more likely associated with some form of "pump and dump" scheme.

Trick #1: The Byzantine General's Dilemma[11]

The purpose of this trick is to allow groups of computers to reach a consensus. This assures the users that the database they are populating is the most valid and recent. Each computer is modeled after a mythical "Byzantine General" in a role-play gaming scenario 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, which has encircled a city that they intend to conquer. In formulating their plan, it is determined that there are only two ways to survive the battle: (1) They all must attack together, or (2) They all must forego the attack and retreat together. Any other combination would result in their 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 generals working for 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 their 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 (n^2).*

Metcalfe’s law can be demonstrated by the advent of previous technologies. For example, a single fax machine is useless, but the value of every fax machine increases with the total number of fax machines in the network, because the total number of people with whom each user may send and receive documents increases. Metcalf’s law provides a means of assessing the value of networks, but also may be broadly applied to the security and fault tolerance of computer networks as well as social networks. In general, this is called the Network Effect

Insurability Test #1

We now apply the three conditions of insurability to the above scenario:

1. Yes, we can identify the risk exposure to the generals and their armies.
2. Yes, citing Metcalfe’s law for networks, the probability of corrupting the network would be inversely proportional to the square of the number of generals.
3. Indeed, the consequences of failure would be tragic, but they are well defined nonetheless

Therefore, Trick #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 generals is to secure the system. Similar strategies are commonplace in engineering applications, such as aircraft, robotics, or any autonomous vehicle where environmental inputs are converted to movements of, say, a flight control surface. The Boeing 777 and 787 use Byzantine proof algorithms, and each are clearly insurable mechanisms in a highly regulated industry of commercial aviation.

Trick #2: Multikey Cryptography

While 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 that they exchange between them. On a decentralized ledger, it is important that the people who are authorized to send information and the people who are authorized to receive that information are secured. It is also important that the information cannot be tampered with in transit. Society now expends a great deal of energy in bureaucratic systems that perform these essential functions to prevent theft, fraud, spoofing, and malicious attacks. Trick #2 allows this to be achieved 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 that Alice has a secret to share with Bob. She can put the secret in a little digital vault and seal it using both her private key and Bob’s public key. She then sends the package to Bob over e-mail. Bob can open the packet with his private key and Alice’s public key. This assures that the sender and receiver are both authorized and the package is secured during transit.

Insurability Test #2

Applying the three conditions of insurability:

1. Yes, we can see the risk exposure to an unsecured message;

2. Yes, we can calculate the probability of failure by examining the strength of the encryption; and
3. Indeed, the consequences of failure could be estimated because the contract would likely represent value.

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

Trick #3: The Time Keeper

Einstein once said, the only reason for time is so that everything doesn't 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, and revision, the date of exchange, etc. Then we must try to manage these individual positions, revisions, and copies moving through the many dimensions of 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 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 "moving background" process: Consider 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 be used only once, and (2) No two vaults can be open at the same time. Acting this out physically is a bit of a chore, but security is assured and there is no way to go backward 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's like guessing the combination to a high school locker. It's hard to do, but once accomplished, everyone can easily see the open locker—that is sufficient proof that work has been done and the block is valid.

Whoever solves the puzzle is awarded electronic tokens called bitcoin. 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 that solve puzzles that keep the train rolling.

Bitcoins (all cryptocurrencies) MUST have value, because if they did not, their respective blockchain would stop cold.

A broken or stalled blockchain would be the cryptocurrency equivalent of bankruptcy. This may account for a fair amount of hype around the value of bitcoins. Many cryptocurrencies enjoy speculative value because they share many characteristics of currency. Not surprisingly, as the price of the token increases, the more secure the blockchain operates.

Insurability Test #3

While this third trick is possibly the most difficult to understand, 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 of the process.

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

The Blockchain Ecosystem[12]

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

Are Cryptocurrencies Money?

There are many prominent articles by many smart people discussing this topic. However, at the time of this writing, article 9 of the Uniform Commercial Code explicitly defines money 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 the loss or destruction of tokens may represent an economic loss, that loss could only be denominated in dollars. The courts and law 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 logic quickly breaks down.

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

Combined Insurability Test

	Insurable
#1 Fault tolerant consensus	✓
#2 Multikey cryptography	✓
#3 Decentralized ledger	✓
Represents money	X
Represents property	X

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 volatility of outcomes rather than reducing it—the exact counter-effect of insurance. If assets can be converted to cryptocurrency, they become difficult to seize or repossess. The extralegal 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. Professional engineering is uniquely positioned and formatted to solve this problem.

Clever legal scholars have suggested that perhaps ownership may be established with a claim against the cryptographic keys that open and close the packets[13]. This is a very interesting idea and something that professional engineers should take seriously because the PE stamp is a form of cryptographic key. We have already established that these nodes and keys are insurable. Logic may be built into key distribution to assign liability or limit liability and thus, price risk correctly.

Part 3: Bridging the Capitalization Gap

In Part 1 we identified the problems that blockchain solves. In Part 2, we identified the problems that blockchains cannot solve. In this part, we will try to specify a bridge that can be built across the chasm over which everyone from banks, entrepreneurs, and autonomous decentralized organizations may cross.

Professional Engineering as a Financial Institution

The professional engineer's fundamental ethical obligation is to hold paramount the public safety, health, and welfare. But in practice, this includes the insurers and banks that assure the public welfare. The Professional Engineering Protocol allows public and private industry to span the capitalization gap—that is, the time gap between the initiation of investment and the delivery of revenue from that investment—in order to borrow money against future revenues. As noted earlier, the US system for licensure of professional engineers (Professional Engineering Protocol) with its own model law, is effective in bridging the capitalization gap—i.e., that long period of time between money flowing to a product or structure and the time that project produces revenue. Within this capitalization gap, the PE stamp holds the asset in suspension during the design and construction phases, serving as a proxy for the finished project on a balance sheet. The Professional Engineering Protocol, in fact, achieves this through many of the same security features as the three tricks of blockchain technology.

1. Professional engineers endure a peer-review process in obtaining and maintaining their license. Examinations qualify the engineers and a revocable license establishes an incentive to high integrity. This bears similarity to the Trick #1; the Byzantine General's Dilemma and the Network Effect.
2. Professional engineers use a common science and language of mathematics as the public key and 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 of trick #2.

3. The professional engineer's stamp acts to finalize a transaction to an indelible legal ledger that memorializes monetary value and title to property. This simulates the time-keeper function discussed in Trick #3.

The continued similarities between the goals of blockchain protocol and the Professional Engineering Protocol are remarkable, thus demonstrating that blockchain ideas are not new and there is nothing to fear. Blockchains may, in fact, be more compatible to existing institutions than previously considered.

Perhaps then, an effective blockchain can be constructed combining components of the physical and the digital domains to achieve the high tolerance for ambiguity that humans provide while also providing the speed, accuracy, and scaleability of computer networks.

For example:

- Instead of a computer modeling a fake network of Byzantine generals, a network of real "generals" can be assembled from a group of licensed engineers 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 that generates a cryptographic key, a professional engineer's stamp could be used as the algorithm to hash cryptographic keys that are authorized to open and close contracts on the blockchain.

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 Insurability of Engineering

Given the insurability of Professional Engineering Protocol and its ability to bridge the capitalization gap, let's now take a look at where we stand on blockchain system insurability:

Insurability Matrix	Blockchain Ecosystem	With Professional Engineering
#1 Fault tolerant consensus	✓	✓
#2 Multi-key cryptography	✓	✓
#3 Decentralized ledger	✓	✓
Represent money	X	✓
Represent property	X	✓

Similarities Between Blockchain Protocol and PE Protocol

Attribute	Blockchain Protocol	PE Protocol
Fault Tolerant	Yes	Yes
Objectivity	Programmed rules and computer algorithm	Engineering laws and principals
Governance	Trusted third party to administer databases	Trusted third party institution to the public, banking, and financial institutions for 100 years
Permanence	Transactions 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 PE 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.

Fig 1: Comparison and similarities between blockchain protocol and the PE protocol. Blockchains can be deployed with strict adherence to existing protocol or by creating hybrids that mix and match components of each protocol to achieve strategic results

Oracle Contracts

A "smart contract" is a decision that is executed by a computer algorithm on a blockchain. For example, if condition A and condition B are triggered, then payment C is executed. An adjudicated smart contract is a smart contract whose execution is contingent on a physical observation or judgment by a reliable witness. The adjudicator would essentially flip the switch that allows the computer to follow a path of logic to, say, approve the next step in a sequence of events; assign, limit, or 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 to forensic standards.

An oracle contract is an adjudicated contract with the added requirement that the adjudicator is deemed the *most appropriate* person to be performing the adjudication. The additional requirement means that a method is required to establish the most appropriate adjudicator—<u>and that method must likewise be insurable</u>. 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 established tangibility, therefore, money and property. Securing the pool of decentralized oracles would be essential to insurability of such contracts on a blockchain. Innovations such as Curiosumé[14][15] would serve that purpose explicitly well.

Banks and insurance companied depend on engineers to verify the design, materials, processes, components, and performance of all subjects that they finance. In general, the construction process consists of 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, and municipal projects cannot be capitalized without professional engineers.

The Professional Engineering Protocol is therefore the best model to start on blockchain because it is already codified in law and proven to be insurable. It will be essential to broaden the breadth and depth of the oracle pool as blockchain implementation advances to include nonlicensed engineers and other makers of useful things, however, the insurability requirements must remain in order for the global blockchain experiment to be ultimately successful.

The Real Value of Engineering

A recent study by the Federal Reserve Bank of San Francisco estimates that each dollar spent on infrastructure results in a $2 increase in GDP (GSP)[16]. Arguably, the GDP is a poor measure of economic activity that does not reflect distribution, multiyear impact, cumulative properties, or intangible assets. For example, a bridge that connects two communities may cost $100 million to create and maintain, but may deliver a billion hours of increased productivity to a community over the 100-year lifespan of the bridge. Society can then invest surplus productivity on such things as art, education, civic activity, raising families, and more engineering. In general, citizens in their community reinvest surplus productivity.

The economic benefit of technological change is difficult to measure. However, in 1957 a study by Robert Solow concluded that between 1909 and 1949, the annual rate of technological change of 1.5% resulted in 90% of the increase in output per capita attributed to that same period. Today such things are complicated to measure, however IHS Inc. published a report that finds that an estimated $3 trillion of additional value has been added to the global gross domestic product, plus another $9 trillion of indirect value in the last 20 years, due to the pace of innovation predicted by Moore's Law[17]. Moore's law simply relates to computer processing speed doubling every 18 months—a fractional proxy for engineering value!

Many engineers now cite conditions where “data engines” may override engineering opinion in many technical and financial decisions such as property valuation, energy policy, land use, infrastructure priorities, resource allocation, and risk management. The 2008 financial crisis was a data problem, not a human productivity problem—the difference between the virtual value of mortgages and the physical value of the asset could not be reconciled in fact. The crisis was precipitated because there was no way to reconcile a virtual asset such as collateralized debt obligations with the physical world of structures and utility. Data is fast and cheap but its value is quickly lost without qualified human observation.

Engineering Contracts

Typical construction contracts, such as those published by the American Institute of Architects and the Engineers Joint Contract Documents Committee[18], provide a framework for the engineer-client interface to engineering projects. EJCDC’s Standard General Conditions of the Construction Contract (C-700), as an example, lays out a long series of requirements that multiple parties need to fulfill in a specific order and within a specific time period. Each may be supplied faster, securely, and more indelibly if filed to a blockchain.

In general, the construction management consists of a long and complicated series of events that all must be contracted, negotiated, ordered, and verified in a secure manner. They are tied together by critical path methodology that is not unlike a blockchain. From the installation of a window wrap in a high-rise residential facility to publishing a flight manifest of a cargo aircraft on a tight schedule, such events can be validated instantaneously and adjudicated on the blockchain by the engineer of record (which is also on the blockchain). The output may be instantly distributed—by a set of pre-programmed rules—to banks, insurance companies, and ground workers—in consensus and without error. Reporting discrepancies, establishing prior art for innovative means and methods, and releasing document revisions, schedule changes, change orders, material orders, or returns are viable applications of blockchain. The engineer would essentially flip the switch that allows the computer to follow an interdependent path of logic.

By flattening the hierarchy and removing bottlenecks, projects can eliminate failure points; compress execution time; reduce volatility; integrate data; and reduce opportunities for fraud, negligence, incompetence, and breach of contract. Engineer-adjudicated contracts can be associated with project milestones and tracked on a master plan for quantity, quality, and chronological order. This data may be combined with the maintenance plan, future renovations, fiscal history, mortgages, loans, valuations, and ultimately the replacement of the project.

Project Lifecycle

In the old days of the automotive industry, the adage held that a new car would lose 25% of its value as soon as it drove off the dealer's lot. Selling a used car was limited to the local classifieds and how much the buyer had in their bank account. Odometer fraud was rampant. In 1984 a computer engineer started CarFax, which brought to the market, by fax machine, a registry of lifecycle events based on public data that could impact the value for a particular vehicle identification number. Since then, the variability in car values has diminished substantially[19]. Carfax has greatly reduced the risk of vehicle pricing while protecting subsequent owners from bad actors and those conditions that undermine the value of the asset. Carfax enables buyers, banks, and insurance companies to accurately identify risk exposures, determine the probability there will be a loss, and determine the consequences of a loss should it occur. Under the leadership of HSI Inc., CarFax is currently introducing a service allowing car owners to track their maintenance records as well.

Bruce Cahan[20], a consulting professor at Stanford's Civil & Environmental Engineering Department in the School of Engineering, is leading a project that accumulates lifecycle data and quality-of-life measures for construction projects using blockchain technology to reduce the volatility in pricing, maintenance, fiscal history, and therefore, property valuation.

During the lifecycle of a building, the design and construction records become part of a total set of documents that describe the asset. These include the property plat, maintenance documents, purchase contracts, insurance contracts, refinance documents, acquisition documents, leases and subleases, mortgages, and documents related to renovations, modifications, and ultimately the building's demolition and replacement. Real estate agents, insurance brokers, escrow services, police, government regulators, vendors, and occupants interact with the structure. Each and every interaction with the building requires some form of contractual agreement and subsequent payout associated with that event. This rich history, or lack of it, can add or subtract value from the property. Today, all of this value is largely invisible, undocumented, and disassociated from the asset.

Keeping track of all this data is prohibitively expensive with current database structures. Using the aviation industry as a comparison, a huge percentage of the costs in aviation is directly associated with documentation, certification, and information control of the aircraft history, performance, and related support infrastructure. The consequences of aviation failures can be devastating, so when an aircraft becomes disassociated from its data; such as operating in a foreign country, or installing counterfeit (uncertified) parts, it can no longer be financed or insured. The value of a $50 million passenger jet may plummet to scrap metal values simply for lack of data. As Cahan states, "The asset becomes the keeper of its own information[21]."

Conclusion

Many of the issues brought up in this report were also present during the time of this author's research on NAFTA and the subsequent Mutual Recognition Document negotiated by the engineering profession in the US, Canada, and Mexico[22]. 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 theory of comparative advantage[23] economic model were, and still are, indisputable. Unfortunately, decentralized markets were administered unevenly, disproportionately, and 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. The difference is that we also have the knowledge, foresight, and the profound responsibilities 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 in blockchain programming 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 that spans the capitalization gap upon which everyone else can travel.

The current path of blockchain deployment, dominated by banks, venture capital, and decentralized autonomous organizations, may not be 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 *recentralizing* databases rather than decentralizing databases—this is what happened to NAFTA. Regulatory arbitrage may serve only to increase volatility and inequality and not decrease it.

The superior method for so-called "controlling" blockchain technology would be through hybrid application of digital and physical proofing mechanisms that are individually insurable so that infinite combinations would still result in easily insurable enterprise. Reinsurance could then provide the ultimate umbrella, diversifying away remaining risk. Unique combinations of such components assigned by entrepreneurs, adjudicated by engineers, and underwritten by banks and insurance companies could yield the new business methods to meet the technical needs of our future at very low cost of capital.

Smart contracts related to physical events must be adjudicated by persons most qualified to do so. For large technology and infrastructure projects, those persons should be licensed professional engineers who flip the switches on the blockchain. Oracle contracts are important and useful only to the degree that the oracles themselves are qualified and decentralized by objective means. The oracle pools may be decentralized through algorithms that convert résumés to cryptography in a manner that secures asset nodes and property titles. Real-world problems can be used as proof-of-work for the puzzles that power blockchains and 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.

It is the opinion of the NSPE FinTech Task Force that the engineering profession can emerge at the apex of the financial and governance value chain if we learn to understand and apply blockchain technology among ourselves. With every technological leap, there is a corresponding period of adjustment. It is essential that engineers proceed with great caution when confronted with any new technology—this is the hallmark of our profession. However, there is also the likelihood that if we do not act quickly enough, or fail to act at all, this new technology could be just as easily used to render the Professional Engineering Protocol obsolete without an adequate substitute that assures the health and welfare of the public.

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

Endnotes

---

[1] McKinsey & Company July 2016 Blockchain in Insurance – Opportunity or Threat, Executive Summary

[2] https://news.coinify.com/5-reasons-bitcoin-important-invention-since-internet/

[3] NSPE Annual Meeting 2015, Seattle; https://www.nspe.org/resources/annual-meeting/bitcoin-protocol-and-future-currency-impact-engineering-profession

[4] https://www.weusecoins.com/en/venture-capital-investments-in-bitcoin-and-blockchain-companies/

[5] Condensed from video by Vinay Gupta, The Ethereum Project. Blockchains, databases, reification: are bottom up standards possible? https://youtu.be/AbacROAa4xY

[6] https://en.wikipedia.org/wiki/Centralisation

[7] https://en.wikipedia.org/wiki/Decentralization

[8] Risk management proof first appeared in National Association of Insurance Commissioners Quarterly Journal August 2016; Author Dan Robles, The Ingenesist Project

[9] http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/

[10] http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

[11] General article and common references on Byzantine Fault Tolerance https://en.wikipedia.org/wiki/Byzantine_fault_tolerance Original paper; The Byzantine General's Problem Leslie Lamport, Robert Shostak, and Marshall Pease

[12] Adapted from video: Patrick Murck on Property Law and the Blockchain, Harvard University, Berkman Institute 2015, https://youtu.be/nqmkAa5VNGc

[13] Patrick Murck, Berkman Center Harvard University

[14] Curiosumé is an application that converts the résumé to cryptography for the purpose of opening and closing adjudicated smart contracts. The Ingenesist Project http://Ingenesist.com. Curiosumé video: https://youtu.be/m_-JkUI5ATE

[15] Curiosumé, at al, currently under development by Quiddity Systems, Indianapolis, Indiana

[16] Federal Reserve Bank of San Francisco http://www.frbsf.org/economic-research/publications/economic-letter/2012/november/highway-grants/

[17] http://press.ihs.com/press-release/technology/ihs says-ramifications-moores-law-lead-trillions-dollars-added-global-econo

[18] Engineers Joint Contract Documents Committee http://www.ejcdc.org/

[19] Adverse Selection due to asymmetric information http://www.dummies.com/how-to/content/how-to-deal-with-adverse-selection-in-managerial-e.html

[20] Bruce Cahan, February 18, 2016, Consulting professor, Stanford University School of Civil and Environmental Engineering

[21] https://goglobal.stanford.edu/profile/bruce-cahan

[22] A Model For The Mobility of Engineers Under NAFTA, Daniel Robles, CETYS University, 1996 http://www.ingenesist.com/wp-content/uploads/2011/03/INCNE596.pdf

[23] https://en.wikipedia.org/wiki/Comparative_advantage

Appendix A

When is a Blockchain Useful?

Adapted from “Avoiding a Pointless Blockchain Project” by Gideon Greenspan

http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

There are times when a blockchain is not the correct database structure for a project, and there are applications where it is. It is important to understand these factors because we will hold the same comparison to engineering applications on blockchain.

If the project does not fulfill the majority of these conditions, one should not be using a blockchain or consider alternate technologies. In the absence of any of the first five, one should consider: (a) regular file storage, (b) a centralized database, (c) master–slave database replication, or (d) multiple databases to which users can subscribe.

Current database technologies have decades of development and have been thoroughly tested. On the contrary, blockchain technology is in its infancy. It is very important to be absolutely clear on why using Blockchain is an advantage. All of the following conditions must exist in order for a blockchain to be the relevant application.

1. Shared Databases
2. Multiple writers
3. Absence of Trust
4. Disintermediation
5. Transaction Interaction
6. Establish Rules
7. Pick the validation system
8. Converting the asset

1. The database

Blockchains are a technology for **shared databases,** i.e., a structured repository of information such as a relational database, containing spreadsheet-like tables or file system. Every transaction on a blockchain represents a set of changes to the database.

2. Multiple writers

Blockchains are a technology for **shared databases with multiple writers**. Blockchains are efficient where there will be multiple people modifying the database. The scalability may be enormous where people, mobile devices, or even sensors (Internet of Things) may write to a blockchain. It is important to identify the writers when specifying the application.

3. Absence of trust

Blockchains are a technology for **databases with multiple non-trusting writers.** This means that one user is not willing to let another modify database entries that it "owns". Similarly, one user will not accept as gospel the "truth" as reported by another user, because each has different economic or political incentives.

4. Disintermediation

Blockchains are a **technology for databases with multiple non-trusting writers to be modified directly.** There is already an effective solution to the problem of non-trusting parties – it is called the trusted 3rd party intermediary – someone who all the writers trust. A blockchain application requires no central gatekeeper or broker to verify transactions and authenticate their source.

5. Transaction interaction

Blockchains truly shine where transactions created by different writers depend on one other. For example, let's say Alice sends some funds to Bob and then Bob sends some on to Charlie. In this case, Bob's transaction is dependent on Alice's one, and there's no way to verify Bob's transaction without checking Alice's first. This is what allows a hand off of 'title' and 'payment' without exposing either party to risk of one party running off with both.

6. Set the rules

Blockchains have the ability to support a set of embedded rules restricting transactions performed. Every transaction can be checked against these rules, and those that fail are rejected. For example, a rule may state that the total quantity of each asset in the ledger must be the same before and after every transaction. This prevents money from being printed out of thin air.

7. Pick your validators

A blockchain's job is to be the **authoritative final transaction log**, on whose contents all nodes provably agree. There are several reasons why this is important. 1. It allows a new user to start from scratch with the most updated version. 2. It does not allow two versions of the database to be in conflict. 3. Blockchains provide precise chronology of events can be proved by comparing two blocks (versions) in a chain of blocks. Users need to have a clear idea of **who your validators are and why you trust them.**

8. Back your assets

What is the nature of the assets being moved around? The question is rather: **Who stands behind the assets represented on the blockchain?** If the database says that I own 10 units of something, who will allow me to claim those 10 units *in the real world*? Who do I sue if I can't convert what's written in the blockchain into traditional physical assets?

http://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/

Appendix B: 2015 – 2016 NSPE FinTech Task Force Projects

Quant: Creation, issuance, and exchange of a Crypto-currency

Part of this project was to create and trade a crypto currency on a blockchain to demonstrate the mechanics of this system. We used the Graphene platform by Cryptonomex on the Bitshares Delegated Proof of Stake Blockchain to create a currency that was then traded among a group of engineers to provide consultation among each other. The Bitshares community was very supportive of our experiment and offered substantial guidance to users such as ourselves who had little prior experience.

We were able to create a digital asset called the Quant. The Task Force chairman was able to distribute Quant to the members of the task force and they were able to pay each other Quant for various activities. This was instructive to demonstrate the ease of use of a blockchain. Watching the dashboard of the Graphene Platform, users could see each block being created approximately 3 seconds apart and they could see their transaction contract appear in the block within seconds of being performed. Users were able to recall the transaction and reveal the time stamp and content. Among the participants in this experiment was an independent engineering witness currently residing in Tokyo. Bernd Nurnberger specializes in the implementation of international process standards and made himself available to witness our interaction. His generous participation was to prove that international transactions performed equally as domestic transactions. Finally, one member of the Bitshares community placed a cash order for 2000 Quant in exchange for 2000 Bitshares, which is a currency trading on a global exchange with convertibility to dollars. While Quant is simply a demonstration, the demonstration proves that Quant can be pegged to a dollar. It is as simple as that.

The NSPE task force discussed the significance of using a blockchain for transactions. Suppose that an engineering firm with 10 engineers received $50,000 dollars in income in a month. Various tasks could have a quant value attached depending on the strategy for completing the projects. The project management could be designed like a game to incentivize various favorable outcomes among players - junior engineers could trade quant with senior engineers for the explicit transfer of knowledge while senior engineers can pay junior engineers to teach them how to use Instragram or Wordpress, for example. The exchange would convert Quant to Dollars so that each engineer can buy what they need in the dollar world. This system may reward collaboration, minimize management, while also assuring product quality, oversight, responsible charge and the formation of communities and professional societies.

By extrapolation, suppose that society needed engineers to design a refrigeration system connects a farm to a grocery outlet. Both the grocer and the farmer would accept Quant because they know that engineers who design refrigeration systems that preserves groceries also accept the currency. Society would desire quant as a currency underwritten by basic infrastructure, which represents real productivity.

For more information see:

Introducing Quant: http://www.ingenesist.com/introducing-quant/

Project #2: The Poor Man's Patent

The concept of The Poor Man's Patent originated in the early days of invention where an inventor could place their idea into a self-addressed stamped envelope. The Post Office date stamp could establish precedence should the idea be copied or stolen. Patent laws changed in about 2013 from "first to invent" to "first to file" making the Poor Man's Patent useless, however, it can still be useful in copyright law, derivation proceedings, and other cases.

Engineers often ask, is there a way to time stamp and store a copy of some intellectual property in anticipation of sharing that work in a proposal, investor meeting, or job interview, etc. Often times, a proposal will require the candidate to reveal proprietary information, or trade secrets, without also providing an NDA from those reviewing the entries, etc.

There could also be a condition where an engineer needs to store a contract that limits liability, asserts dominion over a design or process, or requires controlled access of a draft design. The Poor Man's patent project conducted by that NSPE FinTech task force involved a simple proof of concept taking a real scenario by a task force member.

Using an off-the-shelf open source blockchain application https://blocksign.com/ we were able to upload a document, create a hash of the document and register that on the bitcoin blockchain. The document can now be verified as needed.

The hashes that resulted from this process were:

f03195867d2cde94a8b8e27fe7dd559b
606d62d79d9141470a62ccbbb16df787

The transaction is memorialized in the following Bitcoin Blockchain event:

http://blockexplorer.com/tx/dcc229e51dd860ef26b1daa7bc25a8af59fe0e9bf0dab2ef00b3e5b0d1747556

http://blockexplorer.com/tx/3a3761a866323a37bc07

The above identifiers constitutes proof of ownership and chronology. Applications for professional engineering stamp include the following:

Access management, using a single digital key representing the PE Stamp to access any identity-restricted location, from website single sign-on, to physical buildings, smart vehicles and ticketed locations such as event venues or airplanes.

Automated identification and verification of customers, including Professional Engineers' access to management, organizations, and machinery, either at sign-up or on a real time transactional basis.

Identification and tracking of assets of any form, verifying physical state and/or inspection of vehicles, property, structures and engineering processes.

Transactions, Professional Engineer vetting and permitting of devices or 'Things' to obtain and transact using recognizable and standardized identity, enabling them to manage assets and to securely interact with other devices, people, or organizations.

Digitization of traditional identity components such as professional engineering license, certifications, specializations, education, experience, and peer referrals into a single, versatile digital record.

Adapted from Deloitte paper on blockchain identity proof of concept: http://www2.deloitte.com/uk/en/pages/press-releases/articles/deloitte-launches-smart-identity-proof-of-concept.html