NAMIC
ADVOCACY

BLOCKCHAIN:
WHAT POSSIBILITIES LAY AHEAD FOR PROPERTY/CASUALTY INSURERS

JONATHAN RODGERS
Financial Regulation Manager
National Association Of Mutual Insurance Companies

JONATHAN RODGERS

Jonathan Rodgers serves NAMIC as its financial regulatory manager. Jon is involved in a number of financial and accounting issues, including statutory accounting, risk-based capital, financial examination and analysis, and emerging issues like blockchain and distributed ledger technology. He is part of NAMIC's team covering developments at the National Association of Insurance Commissioners and serves as liaison to national and international accounting organizations.

Prior to joining NAMIC's Government Affairs Department in 2013, Jon served as an accountant in the finance department for more than seven years. Jon is a native of Ann Arbor, Michigan. He graduated from Eastern Michigan University with a bachelor of business administration in accounting. He also has a Master's Degree in finance from Indiana University.

For more information about this NAMIC Issue Analysis please visit www.namic.org/issues/our-positions or contact:

JONATHAN RODGERS
jrodgers@namic.org
317.876.4206

NAMIC is the largest property/casualty insurance trade association in the country, with more than 1,400 member companies. NAMIC supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC members represent 39 percent of the total property/casualty insurance market, serve more than 170 million policyholders, and write more than $230 billion in annual premiums.

TABLE OF CONTENTS

INTRODUCTION

The potential of blockchain to revolutionize the business of insurance is commanding a great deal of attention within the industry. There are many applications for blockchain, most notably as the cryptographic technology that underlies Bitcoin, but there are other uses beyond cash and currency. The Economist attempted to define blockchain in an October 2015 publication as a "way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned."[1] As it applies to insurance, eliminating many redundant, back-office processes or greatly improving the customer experience by way of faster, more efficient claims handling are just two of the benefits that may be realized through blockchain. While blockchain remains in the exploratory phase, many early movers have begun shifting into a proof-of-concept phase as they begin to test products and processes on the blockchain.[2] Now is the time for property/casualty insurance professionals to start looking at the possibilities for future application of this technology to securely share information with policyholders, competitors, suppliers, or others.

The internet arguably has done more to spread knowledge and ideas than any other invention since Johannes Gutenberg's printing press. And, like the printing press, the internet has evolved tremendously since its early days. Thanks to the increased speed with which information was sent, businesses and industries began to leverage the internet, finding ways to provide more value to their customers. No longer could businesses just have a website of their product listings; the next phase required added value such as being able to purchase products or make travel reservations online or live-stream sporting events. Some suggest we are witnessing yet another phase in the development of the internet with the internet of systems, and it will be blockchain technology that will power this development.[3]

This next phase must be capable of processing massive amounts of data in a trusted, secure environment. Blockchain is an innovation with this capability, and it runs on the infrastructure and the network of the existing internet. By allowing digital information to be distributed but not copied, blockchain technology has the potential to be the backbone of a new, secure way of conducting internet-based transactions.

According to Ernst & Young, "Blockchain has the potential to evolve into a core, underlying element in the technology 'stacks' of most P&C carriers, supporting a diverse range of processes and part of your company's future technology 'plumbing.'"[4] This paper outlines the current issues and challenges surrounding the development and use of blockchain. The purpose of this paper is to inform NAMIC members about blockchain, explain how it applies to property/casualty insurance, and categorize the current applications and projects related to the technology. This paper will also explain how insurance companies are currently looking at blockchain, explore some of the use cases and industry consortiums that exist today, and outline the risks and challenges of this technology.

---

[1] "The Great Chain of Being Sure About Things," The Economist, October 31, 2015.
(https://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable)
[2] The Blockchain Insurance Industry Initiative, or B3i, was launched in 2016 to explore the potential use of blockchain to improve back-office efficiencies. The Institutes RiskBlock Alliance blockchain project was created in 2017 and has enrolled dozens of companies to build an insurance blockchain.
[3] Ugur Ozdemir, "Presentation on The Future of Insurance: Blockchain, IoT and Big Data," June 19, 2016. (https://www.youtube.com/watch?v=kcgBPxXAySE&t=630s)
[4] "Blockchain in Insurance," Ernst & Young, 2016. (http://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf)

2

This NAMIC Issue Analysis is brought to you by the NAMIC Advocacy team.

WHAT IS BLOCKCHAIN?

Those in the financial services sector, including the property/casualty insurance industry, are paying close attention to blockchain. At its core, blockchain is a permanent and immutable record of transactions that can be distributed to all participants on a network.[5] These distributed ledgers allow permitted access to data while at the same time protecting it in an encrypted format that complies with privacy regulations.[6,7] In a blockchain there is a series of blocks, each with a timestamp and a link to a previous block, that represent batches of individual transactions. Once transactions are validated they are added to the blockchain in sequence. Essential to a functional blockchain are encryption, redundancy, and immutable storage; therefore, records on the blockchain are considered secure and accurate. In the context of data security, immutable means once data has been written to a blockchain no one, not even a system administrator, can change it. This is good but presents some risks. It is good for auditability, as it would reduce the auditor's role in checking and validating account transactions. Benefits would extend to providers and receivers of data, too, because immutable storage means they can prove that their data has not been altered. However, with immutability comes liquidity risks and, in some cases, solvency risks.[8] Due to the fact that records cannot be altered on a blockchain and are tamper-resistant, when things go awry, it is impossible to reverse a record to rectify the situation. More about the risks and challenges of blockchain technology will be discussed later in the paper.

Another feature of blockchain is it allows people to collaborate on a transaction without having to go through a neutral central authority. It can be used for anything for which people interface with a computer database. Blockchain has the potential to revolutionize industries that rely on reference information providers or transactional data verifiers. It could even potentially

Someone requests a transaction.

The requested transaction is broadcast to a network of computers.

The network **validates** the transaction.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

Once verified, the transaction is combined with other transactions to create a **new block of data for the ledger.**

The transaction is complete.

The new block is then added to the existing blockchain in a way that is **permanent and unalterable**.

---

[5] The word "transaction" represents the transaction of data. This could mean a financial transaction or an exchange of information relevant to a financial transaction (i.e. verification of a physical address or date of birth).

[6] Permitted access refers to the ability to block others from viewing what is on the blockchain; the system is designed to permit or deny access to the blockchain network.

[7] FDA Title 21 CFR Part 11 (1997) defines the criteria whereby electronic records and signatures would be considered trustworthy and reliable. The Sarbanes-Oxley Act provides protection of sensitive data related to financial reporting in public companies. The Payment Card Industry Data Security Standard provides protection of payment card data and related consumer/business details during processing, transmission, and storage.

[8] "Blockchain is Littered with 'Smart' Contracts Gone Bad: Opinion," Insurance Journal, November 16, 2017. (https://www.insurancejournal.com/news/international/2017/11/16/471387.htm)

For more NAMIC Issue Analyses, please visit namic.org/issues/our-positions.

3

eliminate the need for intermediaries, such as agents and brokers, by connecting counterparties directly in a more efficient and secure way. The technology allows for the proof and transfer of ownership or contractual rights without the need for a trusted third party.

To understand how blockchain works, it is helpful to look at the original use case for it. The Bitcoin blockchain is a history of all the transactions that have been agreed upon by the Bitcoin community. Marc Andressen, inventor of Netscape, the first internet browser, said, "Bitcoin gives us, for the first time, a way for one internet user to transfer a unique piece of digital property to another internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate."[9] He has also called blockchain technology "the distributed trust network that the internet always needed and never had."

There are two types of blockchains: permissioned and permissionless. A permissioned blockchain is structured to define which users have access to view or add transactions to a blockchain. In contrast, a permissionless blockchain allows anyone access to add to a blockchain. The focus of this paper will be on permissioned blockchains only, but a brief explanation of some of the underlying technologies, such as cryptography – the computerized encoding and decoding of information – will help to build an understanding of how blockchains work.

When two people want to transact business over the internet, a technology called private key cryptography is needed. This is where each person holds a private key and a public key in order to establish a secure digital identity reference. A combination of public and private cryptographic keys is like a digital signature that is used as a form of consent. Any transaction on a blockchain needs to be signed with a private key. Both permissioned and permissionless blockchains utilize this technology to establish control of ownership by taking the information from the private key and sending it to the network for validation. Both types of blockchains require validators. These validators, or computing nodes, are connected to the blockchain and act as an administrator of the network.[10] The purpose of the nodes is to solve a computational puzzle. The more nodes that are available to validate a transaction, the more secure the network, with one notable exception.[11] In the case of the Bitcoin blockchain, the nodes are incentivized to be the first to solve the puzzle through the chance of being awarded Bitcoins. The network must reach a consensus on each transaction using this mathematical verification process.

One of the alluring features of the Bitcoin blockchain is the amount of computing power it has amassed. Combining this massive computing power with private key cryptographic technology creates a powerful digital exchange system. An example will help illustrate how these technologies work together. Person A is going to send Person B $100. To do this, Person A, using

Each person holds a private key. | Information from the private key is sent to the network for validation. | Validators, or computing nodes, are connected to the blockchain and act as an administrator of the network to solve a computational puzzle. | The more nodes available to validate a transaction, the more secure the network.

[9] "Why Bitcoin Matters," New York Times, January 21, 2014. (https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/)
[10] A node is a computer connected to the blockchain network. It performs the role of validating transactions. It has copy of the most recent blockchain.
[11] "What are Blockchain's Issues and Limitations?" Coindesk – The 51 percent attack: "If more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth. This is called a 51% attack." (https://www.coindesk.com/information/blockchains-issues-limitations/)

This NAMIC Issue Analysis is brought to you by the NAMIC Advocacy team.

his private key, announces he is sending Person B $100 and attaches it to Person B's public key. A block that contains a digital signature, timestamp, and relevant information is broadcast to all nodes in the network. In this example, any computer or node that has access to the network can use its computer processing power to service the network. To do this, the nodes maintain a history of transactions and work to solve proof-of-work mathematical problems.[12] This process is called mining, and when the majority of the miners reach the same answer, a new block is added to the chain and the validation process is complete. Typically, there is an incentive to be the first miner to solve the problem, and, in the case of the Bitcoin blockchain, a single Bitcoin is rewarded to the first miner.

In a multi-key cryptographic system, both parties in a transaction have a public and private key; one party uses her private key with the other party's public key to create a combined key resulting in a "shared secret" or a transaction ready to be validated. A critical component to widespread adoption of blockchain is the deployment of a decentralized identity service. An identity service in a permissioned blockchain is most applicable to insurance companies as it allows for businesses to gather appropriate information on cryptographic keys used by customers and businesses to digitally sign-off on transactions. Deploying identity management on the blockchain could eliminate or significantly reduce fraud. For example, by storing customer information or claims history on the blockchain it would make it extremely difficult to file a claim more than once. Criminals would need to find another way to mask their identities if they want to manipulate the blockchain.

Anyone with the appropriate encryption rights can access a copy of the blockchain. This allows regulators, including insurance regulators, the ability to verify past transactions without having to trust the participants in the original transaction.[13] Transactions are recorded without revealing the contents of the transaction to the public.[14] Since participants have appropriate encryption rights and access to a copy of the digital ledger, they act as a common source of truth. Once validated, each block is added to the blockchain in sequence linking it to all previous blocks, making it impossible to falsify a transaction and resulting in a complete audit trail being maintained. The system is designed so that these blocks cannot be removed or manipulated.

[12] Proof-of-work is a piece of data that is difficult (costly, time-consuming) to produce but easy for others to verify.
[13] Trust has already been established. Since the blockchain cannot be altered without the network being notified, trust has been established that regulators can rely on.
[14] This is done using hash-functions, which, much like human fingerprints, verify that the hash matches a specific person. Most importantly, one cannot "back into" or identify a person based on a recorded hash; you can only verify that a hash matches.
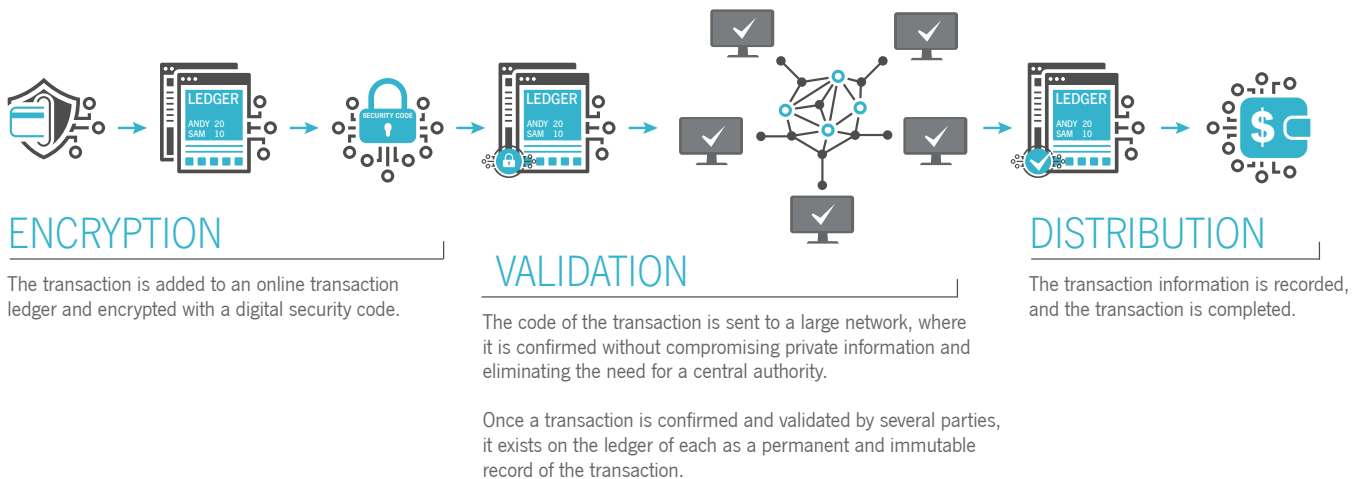
All nodes or participants on a blockchain have the most recent version of the truth, or the most recent version of the blockchain, because once a block is finalized, or mined, it cannot be altered.[15] However, there is a risk with a single node or a group of nodes gaining a majority of the computing power on the network. A group of miners that controls a majority of the computing power, more than 50 percent, would be able to prevent new transactions from gaining confirmations. This is because once a block is mined, the majority of the miners must come to the same answer and reach a consensus before the validation process is complete. These nodes are essentially voting with their computing power, and when more than 50 percent reach a consensus, it adds a new block to the chain that is timestamped. While this clearly is a vulnerability, it is all done in a transparent way. A network that rejects new transactions or blocks other users' transactions would quickly suffer a loss of confidence.

What Andressen and many others see in blockchain technology is similar to what forward-thinking companies were considering in 1996 with the World Wide Web. They saw great potential but knew it was far from adoption at scale. The key to successfully implementing a common blockchain is to build a network that is trustworthy and transparent. As Andressen alluded, the internet needs a "distributed trust network" and that is what blockchains can provide. Consumers put a lot of trust in the internet when they purchase products online; they assume credit card information will not be compromised. They trust medical information is safe when they access online records from their insurance companies. However, the frequency and severity of data breaches are increasingly jeopardizing that trust in the system. Data breaches or hacking events are commonplace today, as evidenced by the massive Equifax hack.[16] Blockchain offers the possibility to enhance the trust the public puts in the internet and do it in a more secure, transparent, and cost-effective manner.

In a nutshell, blockchain is a system where everyone shares the same database. It establishes a framework for a single version of the truth that is shared with the network, enabling faster, more accurate, and efficient processes.

ANATOMY OF A TYPICAL BLOCKCHAIN TRANSACTION
Here is a step-by-step breakdown of how a transaction between two parties occurs algorithmically via distributed ledger technology.

ENCRYPTION
The transaction is added to an online transaction ledger and encrypted with a digital security code.

VALIDATION
The code of the transaction is sent to a large network, where it is confirmed without compromising private information and eliminating the need for a central authority.

Once a transaction is confirmed and validated by several parties, it exists on the ledger of each as a permanent and immutable record of the transaction.

DISTRIBUTION
The transaction information is recorded, and the transaction is completed.

---

[15] If any one node has a different version of the truth, it would be quickly spotted and rejected by the other network users.

[16] Equifax says the breach exposed Social Security numbers and other data from 143 million Americans. The theft obtained consumers' names, Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers.

WHO IS INVESTING IN THIS TECHNOLOGY?

Whether it be the U.S. Defense Advanced Research Projects Agency investigating[17] ways to create an unhackable messaging system or Walmart experimenting[18] with technology to enhance food safety, blockchain is being explored by a wide range of organizations and is attracting billions in venture funding. According to CoinDesk, between 2015 and 2016 nearly $1.1 billion in venture capital was invested in blockchain technology.[19] In 2017 blockchain entrepreneurs raised $350 million in venture capital funding; however, an additional $1.38 billion was raised through initial coin offerings.[20]

According to McKinsey & Company investments in blockchain technology by the insurance sector is expected to grow at a 59% annual rate until 2019. Major insurance companies are investing big money into the technology already. For example, AXA, a French multinational insurance firm headquartered in Paris, invested about $55 million[21] into a blockchain startup in February 2016.[22] AIG, a New York-based international insurance company, is beyond the exploratory phase and has moved on to testing real products in the market; it issued its first insurance policy based on blockchain technology in June 2017.[23] Then there are startups like InsurETH, a blockchain-based travel delay insurance company that automatically detects if its users have flight delays. If there is a flight delay, the app triggers an insurance claim that is verified on the blockchain ledger and automatically pays the claim if proven correct.

Those investing in blockchain see the value in participating in this ecosystem, but more importantly, they see opportunities. There are opportunities to improve efficiency and customer experience. They see the opportunity to lower the costs of transaction processing while increasing trust between parties. In a Deloitte survey of more the 300 U.S. executives, more than 25 percent of the respondents indicated they view blockchain as a critical, top-five priority; however, approximately 33 percent view the technology as over-hyped.[24] In the same survey, 28 percent of the respondents said their company had invested $5 million or more in blockchain technology and another 10 percent had invested $10 million or more. Of the 300 respondents, 39 percent indicated they had little or no knowledge about blockchain and only 12 percent of financial services respondents indicated they have deployed blockchain into their operations.

In a similar survey of global insurance businesses conducted by PricewaterhouseCoopers, 68 percent of participants expect to adopt blockchain as part of an in-production system in 2018, up from 20 percent in 2017 and 2 percent in 2016.[25] This demonstrates that widespread adoption of blockchain technology in the insurance industry in upon us. Both surveys seem to indicate that financial services are behind industries like technology, telecommunications, and manufacturing when it comes to blockchain; however, the results of the PwC survey suggest that insurance is starting to emerge as the leader among the financial services industry when it comes to blockchain adoption.

[17] "Not Just Bitcoin: Why The Blockchain Is A Seductive Technology To Many Industries," NPR, May 4, 2016.
(https://www.npr.org/sections/alltechconsidered/2016/05/04/476597296/not-just-bitcoin-why-blockchain-is-a-seductive-technology-to-many-industries)
[18] "IBM Forges Blockchain Collaboration With Nestle & Walmart In Global Food Safety," Forbes, August 22, 2017.
(https://www.forbes.com/sites/rogeraitken/2017/08/22/ibm-forges-blockchain-collaboration-with-nestle-walmart-for-global-food-safety/#6ce589623d36)
[19] "Blockchain Venture Capital" Coindesk. (https://www.coindesk.com/bitcoin-venture-capital/)
[20] "$1.6 Billion: All-Time ICO Funding Climbs as Record $500 Million Invested in July," Coindesk, August 4, 2017.
(https://www.coindesk.com/1-6-billion-all-time-ico-funding-climbs-as-record-500-million-invested-in-july/)
[21] "AXA Strategic Ventures Invests in Blockchain Technology," AXA website, February 4, 2016. (https://group.axa.com/en/newsroom/news/axa-strategic-ventures-blockchain)
[22] "Blockchain Technology in the Insurance Sector," McKinsey & Company, January 5, 2017.
(https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf)
[23] "AIG 'Smart' Policy Uses Blockchain to Manage International Coverage for Bank," Insurance Journal, June 15, 2017.
(https://www.insurancejournal.com/news/national/2017/06/15/454457.htm)
[24] "Deloitte Survey: Blockchain Reaches Beyond Financial Services with Some Industries Moving Faster," Deloitte website, December 13, 2016.
(https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-survey-blockchain-reaches-beyond-financial-services-with-some-industries-moving-faster.html)
[25] "Insurance's New Normal: Driving Innovation with InsurTech," PwC website, 2017. (https://www.pwc.com/gx/en/industries/financial-services/fintech-survey/report/insurance.html)

For more NAMIC Issue Analyses, please visit namic.org/issues/our-positions.

7

BLOCKCHAIN SOLUTIONS FOR PROPERTY/CASUALTY INSURANCE COMPANIES

With the proliferation of technologies that are connected to the internet, such things as wearables, drones, telematics, or any of the myriad devices known as the Internet of Things, blockchain could potentially enable and support the significant digital transformation currently underway in the property/casualty insurance industry.[26] Much of this transformation relies on data and the IoT devices that track these data. These technologies and others are proving to be reliable sources of data. If properly implemented, the value creation potential of blockchain technology for the property/casualty insurance industry could be immense.

In the following section, we'll review many of the projects and concepts that insurance companies and startups are working on related to blockchain technology. This will demonstrate why actuaries and underwriters are looking at blockchain and big data to build models that more accurately predict outcomes, resulting in more accurate pricing. Some projects include smart contracts that are being used to manage and settle claims. In addition, some are working on blockchain solutions that may reduce or eliminate fraud by changing the process for handling claims. All of this could lead to better customer experiences and a reduction in claims processing costs.

THE INSTITUTES

The Institutes, a leading education provider for the property/casualty insurance industry, is emerging as a leader in the blockchain space. In July 2017, it launched a blockchain consortium with the goal of developing use cases for the technology.[27] The consortium is called the RiskBlock Alliance comprised of 30 members across the property/casualty value chain. The group is working on solutions ranging from proof of insurance, subrogation, data sharing and risk registries, and parametric insurance. The Institutes is also a founding member of the Enterprise Ethereum Alliance, a cross-industry group that is working to develop standards and protocols for use on the private Ethereum networks. Ethereum is one of several distributed computing platforms that make up the blockchain ecosystem.

In August 2017, the Institutes' RiskBlock Alliance held a workshop that allowed members to share their perspectives on blockchain technology.[28] The group, which includes several NAMIC members, believes that blockchain technology will be disruptive and that industry cooperation is needed to manage through this disruption. Peter Miller, president and chief executive officer of The Institutes, agrees: "collaboration and progress on proof-of-concept use cases demonstrated during the RiskBlock workshop are further validation that there is significant industry support behind both the consortium and building a truly robust insurance blockchain application."

FRAUD DETECTION AND RISK PREVENTION

The Insurance Information Institute estimates that 10 percent of the property/casualty insurance industry's incurred losses and loss adjustment expenses each year can be attributed to fraud.[29] This amounts to about $34 billion per year. As

[26] "How Blockchain Could Revolutionize the Internet of Things," Forbes, June 27, 2017. "Blockchain is promising for IoT security for the same reasons it works for cryptocurrency: It provides assurances that data is legitimate, and the process that introduces new data is well-defined." Ahmed Banafa, IoT expert and lecturer at San Jose State University.
[27] "The Institutes Announces Formation of RiskBlock: The Blockchain Consortium for the Risk and Insurance Industry," The Institutes website, July 12, 2017. (https://www.theinstitutes.org/about-us/media-center/articles/institutes-announces-formation-riskblock-blockchain-consortium-risk)
[28] "The Institutes RiskBlock Alliance Conducts Workshop to Promote Blockchain in Insurance," The Institutes website, August 15, 2017. (https://www.theinstitutes.org/about-us/media-center/articles/institutes-riskblock-alliance-conducts-workshop-promote-blockchain)
[29] "Background on: Insurance Fraud," Insurance Information Institute website, November 6, 2017. (https://www.iii.org/article/background-on-insurance-fraud)

This NAMIC Issue Analysis is brought to you by the NAMIC Advocacy team.

mentioned earlier, deploying identity management on the blockchain would enhance the overall capabilities of the technology, which requires cooperation between the insurance industry and all other relevant parties. For example, to validate the authenticity of documents, such as medical records, the insurer would need to be granted access to those records, and those records would need to be on the blockchain. Such cooperation is required for the full potential of blockchain to be reached.

With blockchain, there is complete transparency of transactions, making it easier to detect fraudulent activity.[30] The redundancy built into the blockchain is achieved by retaining a complete historical record of every transaction. This gives it the ability to identify possible fraudulent or duplicate claims. This is because all transactions (in this case, claims) are on the blockchain, which is shared in the network and verified by the participating insurers.

SECURITIES SETTLEMENT

There is a lack of beneficial ownership tracking in the securities industry, and companies like Symbiont.io are working on blockchain solutions that will eventually lead to investors actually owning the stocks or bonds in their brokerage accounts.[31] Caitlin Long, former chairman and president of Symbiont.io, spoke to the National Association of Insurance Commissioners in December 2016 about the lack of beneficial ownership tracking and how this solvency risk impacts insurers.[32] "In the old days during regulatory exams, insurance regulators used to audit the paper certificates held in insurers' vaults to verify that securities recorded on Schedule D were actually there. This is no longer possible to do today, owing to the indirect manner of securities ownership and the use of omnibus accounts by layers upon layers of securities industry intermediaries."

Today investors do not legally own the securities in their brokerage accounts; they are beneficial owners, and there is an enormous intermediary that legally owns the shares. Nearly all publicly owned securities are owned by Cede & Co., which is a nominee of the Depository Trust Co. This creates a large, although low-probability, counter-party risk. For each security, Cede & Co. owns a master certificate, and transactions are recorded as debits and credits to DTC members. Members include more than 600 broker-dealers and banks. Similar to the structure of the banking industry, the assets in a brokerage account have been lent to the brokerage firm that lent those to a custodian that borrowed them from the DTC.

Companies like Dole Foods know very well the problems that can arise when there is a lack of beneficial ownership tracking in the securities industry. In February 2015, a Delaware Chancery Court ordered Dole shareholders to submit a form for their claim on a class-action lawsuit; the claims Dole got back were for 49 million shares; however, this number exceeded the 36 million shares outstanding. These were all legitimate valid claims. Unfortunately, Dole Foods is not the only example of the problem. This example highlights a problem with the lack of beneficial ownership tracking in the broker/dealer community and a solution to the problem is one that the community needs to resolve.

Blockchain technology has the potential to be the solution to the lack of beneficial ownership tracking in the securities industry. Delaware has started the Delaware Blockchain Initiative as an effort to clean up the back office of Wall Street. Symbiont.io is a technology partner to that effort and was instrumental in getting Delaware onboard with blockchain technology. In 2017, Delaware amended its corporate law to permit distributed ledger registrations in Delaware – a very important state when it comes to corporate law – almost 85 percent of new registrations for corporations happen there. There is a rich history of corporate law and litigation history surrounding the exact requirement of administering a corporation. Once a company is

---

[30] "Blockchain in Insurance," Ernst & Young, 2016. (http://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf)

[31] Caitlin Long, "Presentation on What Blockchain Means," April 6, 2017. (https://www.youtube.com/watch?v=UxFyXKLazlQ&feature=youtu.be)

[32] Caitlin Long's Speech to Insurance Regulators: "Fixing a Fixable Solvency Risk to Insurers," Symbiont.io website, December 12, 2016.
(https://symbiont.io/blog/2016/12/12/caitlin-longs-speech-to-insurance-regulators-fixing-a-fixable-solvency-risk-to-insurers)

For more NAMIC Issue Analyses, please visit namic.org/issues/our-positions.

9

registered on a distributed ledger, there is no piece of paper that can sit at the DTC; therefore, it completely changes the plumbing of the securities industry and allows record owners to be beneficial owners of shares again. This would prevent the Dole situation from occurring.

REINSURANCE

The Blockchain Insurance Industry Initiative, or B3i, launched in October 2016 with the goal of determining the viability of using distributed ledger technology in the insurance industry. There are 15 founding member companies that are on the verge of developing a reinsurance product that will be administered entirely on the blockchain.[33] The product, still in its testing phase, is a reinsurance property excess of loss contract that was initially put to the test in September 2017. Going into testing, an ideal outcome during this proof-of-concept phase would be for the blockchain to control the transaction, from when the reinsurance is posted to when a claim is settled. The blockchain would facilitate payments for premiums and claims that are reported and settled.

Members of the B3i are committed to driving insurance and reinsurance transactions into a common blockchain standard. As the group settles in on more use cases, it is anticipated that its blockchain will reach a critical mass that will lead to standardization. There is great interest from others in the industry that want to join B3i; some 50 firms have approached B3i in 2018 asking how they can join the industry consortium. In October 2017, 23 new entrants joined B3i following the successful launch of its reinsurance market prototype. The new members of the group will participate in beta testing. This will involve running the contract on the blockchain in an environment conducive to testing new business models, what might be referred to as a sandbox environment.[34]

The group of founders have brainstormed many ideas to apply blockchain technology. The general theme that emerged during these discussions was the industry takes too long to settle transactions. Cross-border payments are too cumbersome. A reinsurance transaction is international in nature, particularly for large insurance carriers, and is a business-to-business transaction; therefore, B3i considers reinsurance to be the easiest use case to develop a common consensus on standards. As the group develops use cases and other proofs-of-concept, all ideas will be centered on four key pillars:[35]

Working capital – The focus is on certainty about when cash will flow and due dates when premium is collected and claims are paid.

Optimization of foreign exchange efficiencies – Insurance is a cross-border global business and foreign exchange transactions are not cost-effective.

General operational efficiencies and risk reduction – Companies will reduce operational risk by improving processing speed. Pushing paper and data back and forth, the lack of standard data, and too much redundant reconciliation are sources of operational risks.

Data integrity improvements – Utilizing Association of Cooperative Operations Research and Development standards and putting ACORD on a standard platform will bring improved data integrity and quality. ACORD is a non-profit organization that provides the global insurance industry with data standards and implementation solutions.

---

[33] "Blockchain Industry Initiative, B3i, Expands with 23 New Broker, Re/Insurer Entrants," Insurance Journal, October 2, 2017. (https://www.insurancejournal.com/news/international/2017/10/02/466117.htm)

[34] A similar concept is a regulatory sandbox. This allows for the testing of new business models that are not protected by current regulation or supervised by regulatory institutions. Munich Re submitted a proposal to the NAIC for a regulatory sandbox in 2017 with the goal to lower the barriers for testing of new ideas and to ensure the risks are not transferred from businesses to consumers.

[35] "B3i – Turning Blockchain Use Case into Business Case," Paul Meeusen, April 6, 2017. (https://www.linkedin.com/pulse/b3i-turning-blockchain-use-case-business-paul-meeusen/)

These four pillars will help B3i measure the performance of its first blockchained reinsurance product, as well as all future proofs-of-concepts deployed on the blockchain. While the group has just launched its first product, there is a long line of use cases across the 15 members that they have started to prioritize. Paul Meeusen, Munich Re's representative on B3i, said, "There is really no limit across the value chain, starting with the private policyholder – the individual – all the way to the reinsurer."[36] The different legal and regulatory constraints in each country will be a challenging aspect to navigate when it comes to primary insurance.

SMART CONTRACTS

Smart contracts are one of the most promising applications of the blockchain.[37] They are computer programs that run on top of the blockchain. Essentially, the terms of the contract are put on the blockchain, albeit in code form, and shared between all participants. The contract automatically performs across all counterparties based on pre-defined rules. Verified data sources, or so-called oracles, cryptographically attest to the origin of the data and push the information to the smart contract. For example, an insured farmer has a smart contract, and a claim is triggered when drought conditions are reported by a verified weather database. In this example, the oracle would be the National Weather Service database.

Smart contracts on the blockchain are distributed to all participants and accessed on a permissioned basis. Not only do smart contracts define the rules for an agreement, they also automatically enforce those rules. Automated claims payment processes integrated with third-party vendors will lead to better customer outcomes. Policyholders will get paid faster, and the insurer will have lower claims processing costs. Situations where the parameters for payment are clear or there is little probability for disagreements is where smart contracts will likely first be deployed in the insurance space.
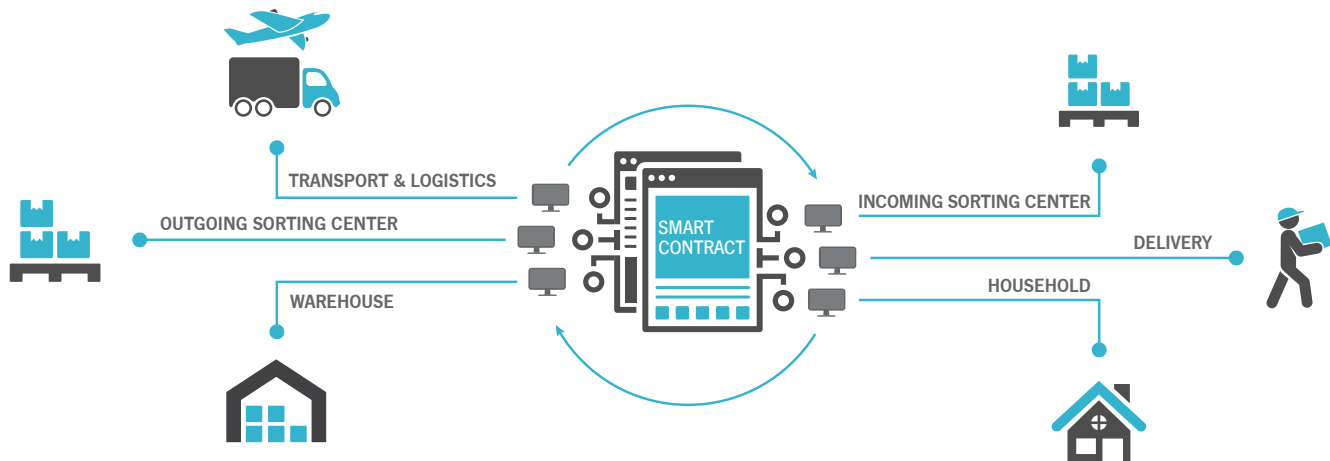
[36] "Brave New World: 1st Reinsurance Product Heads to the Blockchain," Insurance Journal, June 9, 2017.
(https://www.insurancejournal.com/news/international/2017/06/09/453984.htm)
[37] "Blockchain Accelerates Insurance Transformation," KPMG White Paper, 2017.
(https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/01/blockchain-accelerates-insurance-transformation-fs.pdf)

IoT/BIG DATA

By 2020, there will be more than 20 billion connected devices; this will result in an explosion of data.[38] Most of these devices do not have the necessary security in place; however, these challenges can be overcome using blockchain technology. The current IoT ecosystem identifies, authenticates, and connects all devices through cloud servers.[39] Companies are working to build standards around the way IoT devices exchange and make use of information. The company Chronicled is open-sourcing a tool for registering connected devices and is using the Ethereum blockchain to make private IoT database registries interoperable.[40] Like Bitcoin, the Ethereum system is built on a blockchain in which every transaction is recorded publicly. But unlike Bitcoin, Ethereum has the ability to provide programmable transactions known as smart contracts.

Ultimately, these devices will need to talk to each other, but most importantly, they are going to need to trust one another. The devices or machines will need to have identities and will have to make decisions on whether or not to trust other devices. Blockchains are the vehicle to enable a machine-to-machine economy. Verifying the identity of a device in a secure and public way is the first step.

PARAMETRIC INSURANCE

By pairing parametric insurance with blockchain-based smart contracts, insurers can offer lower cost products and participate in new markets. Many of the most common insurance contracts are simply if/then statements that can be digitized as blockchain-based smart contracts. In its most basic form an insurance contract is an agreement to make payment upon the occurrence of an event. Parametric insurance is a form of insurance based on objective measures, such as the magnitude of a weather event.[41] Payouts are determined using objective indicators that serve as an effective proxy for the type of loss being covered. It is most commonly used for natural catastrophes, like hurricanes and tornados, when specific damage is difficult to calculate and costly to administer. Instead of using claims adjusters to survey the damage, parametric insurance utilizes pre-defined parameters to enable blockchain-based smart contracts, reducing the administration costs associated with claims payout.

HOW DOES PARAMETRIC INSURANCE WORK?
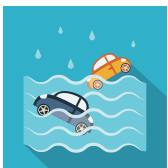
Parametric Insurance is based on an independent parameter or index that is correlated to client's losses.

e.g. temperature, wave height, wind speed, etc.
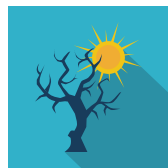
Once a threshold is reached payment is triggered automatically.

e.g. wind speed 10% below 5-year average.

This product offers a seamless customer experience with an optimized insurance process and amplifies the scope of the insurable.

---

[38] "IoT Devices Will Outnumber the World's Population This Year for The First Time," ZD Net, February 7, 2017. (http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/)

[39] "Decentralizing IoT Networks Through Blockchain," Tech Crunch, June 28, 2016. (https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/)

[40] "Blockchain Startup Chronicled Launches Ethereum IoT Registry," Coindesk, August 24, 2016. (https://www.coindesk.com/blockchain-startup-chronicled-launches-ethereum-iot-registry/)

[41] "Smart After All: Blockchain, Smart Contracts, Parametric Insurance, and Smart Energy Grids," Alan Cohn, Travis West, and Chelsea Parker, April 25, 2017. (https://perma.cc/TY7W-Q8CX)

Because claims adjusters would no longer be necessary in a parametric insurance environment, insurers will be able to enter new markets where previously they needed a local claims adjuster. This will also allow insurers the ability to offer products at a lower cost. Because of the low cost to service these types of products, insurers may start to offer lower-premium products. Typically, these products are not offered because they are not profitable for insurers, but with lower transactional costs, these products may become attractive to sell.

The key to a successful parametric insurance program is to find the right measures that can serve as effective proxies for the losses being covered. Blockchain-based smart contracts that are administered through oracles present incentives for insurers to find more ways to parameterize other policy structures. By monitoring smart contracts in real-time with the use of analytical software, insurers will be able to examine the record of transactions and loss occurrences, therefore, getting better information about the effectiveness of the proxies in use.

CLAIMS MANAGEMENT

Claims management and prevention are other areas where insurers can benefit from blockchain technology.[42] Imagine the costs an insurer could save if it could automatically verify coverage, determine if payment is required, and if so pay the policyholder. Claims could be verified and handled almost instantly by providing real-time access to verified data sources. Claims can be submitted using a mobile phone or sensors that are connected to the internet and transmit data to the blockchain. Loss adjuster costs would be reduced since the blockchain would facilitate the communication and coordination among all parties. Customers would be happier with the faster service.

In terms of loss prevention, consider how sensors are used to trigger alerts by the following example of how the technology could be utilized. A driver who has a telematics device in his car gets into an accident. At the moment of the crash, a new claim is initiated followed by a series of action alerts – for example, relevant data is sent to local medical teams and towing service companies and/or repair shops. The blockchain is a network that allows for these "participants" in the process to be alerted about the claim and to have all the relevant information they need in real-time. Today, the amount of duplication that happens from initial claim filing to final claim payment is not trivial. There is much manual data entry by multiple parties of the same information. This duplication could be eliminated if claims were settled using smart contracts. If coverages were automatically verified and payments for repairs were automatically made once validated by an authorized repair shop, then contract disputes would be significantly reduced.

DIGITAL IDENTITIES/RECORDKEEPING/ONBOARDING

People are concerned with losing control of their personal data when they give it to a company. A customer-controlled blockchain for identity verification would eliminate the need for customers to enter personal data over and over again; businesses would benefit with customer recruiting and onboarding if the data entry process was eliminated. Errors would be reduced. If data stored on the blockchain is accessible to customers, they can monitor who viewed their records and at what time they were accessed.

Personal data isn't stored on the blockchain; only its verification is registered on the blockchain. There are solutions being worked on related to Know-Your-Customer data. Currently, the process of onboarding a new customer at a financial institution

---

[42] "Blockchain in Insurance," Ernst & Young, 2016. (http://www.ey.com/Publication/vwLUAssets/EY-blockhain-in-insurance/$FILE/EY-blockhain-in-insurance.pdf)

For more NAMIC Issue Analyses, please visit namic.org/issues/our-positions.

13

involves an employee filling out KYC forms and gathering information in an inefficient and time-consuming manner.[43] Deloitte is working on a KYC model that works with service providers that would be authorized to perform KYC checks for customers who would like to be onboarded by a financial institution, such as an insurance company. Blockchain can eliminate the need to repeat the full identification and verification process to onboarding, reducing compliance costs for insurance companies. With KYC, customers can grant access to a company for identity data to be verified and then forward the verified identity data to other companies, avoiding the need to repeat the process.

RISKS AND CHALLENGES TO BLOCKCHAIN TECHNOLOGY

The potential for blockchain technology is clear with many people anointing blockchain as a revolutionary technology. Yet, as with all new technologies and innovations there are risks and challenges that must be overcome and addressed in a meaningful way. Questions arise such as: How do you assure protection against hacks? Who is involved in correcting and identifying coding errors? What is the blockchain governance[44] process?

To understand the risks involved with blockchain technology, one needs to look no further than the recent demise of the Decentralized Autonomous Organization, an Ethereum-based smart contract startup created to act as a funding vehicle. The DAO was hacked and funds were withdrawn from it when hackers exploited the splitting function.[45] Essentially a coding error in the design of the smart contract caused the hack and the loss of one-third of its total funds.

Risk of problems arising from both the automated nature of blockchain technology as well as the people developing the smart contracts is evident in the demise of the DAO. It is also a reminder that the technology is still in the developing stages and that more failures will come, so testing the technology is critical.[46] It is easy to get excited about the potential of smart contracts powered by the blockchain, as smart contracts by their design are predictable. However, until the code is released to the world, the only thing known for certain is how the code will react based on the inputs that have been tested. Just like any system, people can be the problem, and, as evidenced, an oversight during coding can have disastrous results.

The DAO is a reminder of how nascent the blockchain ecosystem remains and how regulatory oversight and consumer protections will need to be addressed in this new environment. Lessons have been learned – for instance, disaster recovery plans and procedures are critical before deploying this technology. As well, coding, much like law, evolves as events are experienced. Critical to making blockchain widely applicable is a fully developed technology.

---

[43] Deloitte's RegTech Offering: Blockchain-Powered KYC-as-a-Service Solution," Bitcoin Magazine, May 10, 2017. (https://bitcoinmagazine.com/articles/deloittes-regtech-offering-blockchain-powered-kyc-service-solution/)

[44] Fred Ehrsam, co-founder of Coinbase, "As with organisms, the most successful blockchains will be those that can best adapt to their environments. Blockchains may teach us more about governance in the next 10 years than we have learned from the 'real world' in the last 100 years."

[45] "The DAO, The Hack, The Soft Fork and The Hard Fork," Cryptocompare.com, January 18, 2018. (https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/) From the article: "The DAO was created with an 'exit door' known as the 'split function.' This function allowed users to revert the process and to get back the Ether they sent to the DAO. If somebody decided to split from the DAO, they would create their own 'Child DAOs' and approve their proposal to send Ether to an address after a period of 28 days. The attack happened due to an exploit found in the splitting function. The attacker/s withdrew Ether from the DAO smart contract multiple times using the same DAO Tokens. This was possible due to what is known as a recursive call exploit. In this exploit, the attacker was able to 'ask' the smart contract (DAO) to give the Ether back multiple times before the smart contract could update its own balance."

[46] "Blockchain is Littered with 'Smart' Contracts Gone Bad: Opinion," Insurance Journal, November 16, 2017. (https://www.insurancejournal.com/news/international/2017/11/16/471387.htm)

This NAMIC Issue Analysis is brought to you by the NAMIC Advocacy team.

Regulatory and legal questions arise, such as who owns blockchain? Will regulators trust the process? What will happen if a policyholder or claimant identifies errors in or harm from blockchain transactions? Will bad faith apply? Will insurers pull back their reliance on the blockchain if these struggles arise? Do technical standards need to be adopted? All of these questions will need to be considered.

Finally, privacy and security concerns are a challenge for many. Before anything is widely accepted all security vulnerabilities must be identified and corrected. Hackers view new technology as an opportunity, and cybersecurity is less understood with new technologies. While private and permissioned blockchains and encryption exist, cybersecurity concerns must be addressed before the population is comfortable that personal data is secure on the blockchain.

CONCLUSION

Blockchain technology is still in the early stages of development as different industries, including property/casualty insurance, are researching and testing use cases and proofs-of-concept. Regulators and legislators, too, are learning more about the technology and are conducting studies and developing initiatives to aid in their education. Infrastructure and computing power are being built up to support the blockchain platform – the amount of data and participants that could potentially be part of the blockchain ecosystem will require immense amounts of storage space and computing power.

Today there are many people considering the possibilities of the technology and a few are even building out the insurance blockchain. The time is now for property/casualty insurance professionals to review the potential value creation opportunities and the possible cost savings based on the future application of this technology. Through the secure sharing of information, blockchain technology may well be the solution to the industry's high expense ratios and may be the way the industry thrives in an increasingly technological society.

For more NAMIC Issue Analyses, please visit namic.org/issues/our-positions.

15

NAMIC

NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES