

Blockchain Opportunities for Insurance and Financial Industries

March | 2023

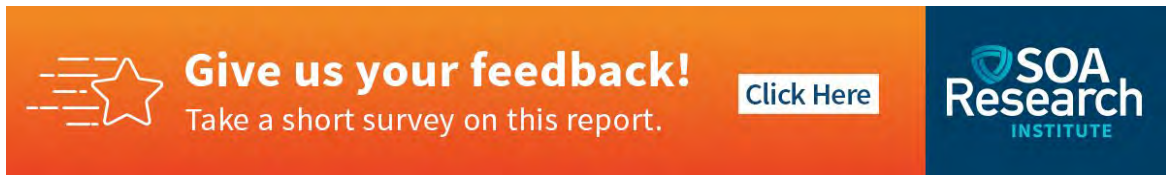




Blockchain Opportunities for Insurance and Financial Industries

A workshop bringing together research and business applications

AUTHORS Gwen Weng, FSA, CERA, FCIA, CFA

SPONSOR Actuarial Innovation and Technology
Strategic Research Program Steering
Committee

A horizontal banner with a gradient background from orange to dark blue. On the left, there is a white star icon with horizontal lines extending from its left side. To the right of the star, the text "Give us your feedback!" is written in white, bold font, followed by "Take a short survey on this report." in a smaller white font. Further right, a white rectangular button with the text "Click Here" in blue is present. On the far right, the SOA Research Institute logo is displayed in white and blue.

 **Give us your feedback!**
Take a short survey on this report. [Click Here](#) 

Caveat and Disclaimer

The opinions expressed and conclusions reached by the authors are their own and do not represent any official position or opinion of the Society of Actuaries Research Institute, the Society of Actuaries or its members. The Society of Actuaries Research Institute makes no representation or warranty to the accuracy of the information.

Copyright © 2023 by the Society of Actuaries Research Institute. All rights reserved.

CONTENTS

- Executive Summary 4**
- Section 1: Introduction 5**
- Section 2: Blockchain Insurance Application and Blockchain Risks 6**
 - 2.1 Peer-to-Peer Insurance 6
 - 2.2 Loss Modeling 6
- Section 3: Current Projects of Interest..... 8**
 - 3.1 Current AZ BARC Projects 8
 - 3.2 Zero Knowledge Proof and its Applications 9
- Section 4: Panel Discussion 12**
 - 4.1 Arbol..... 12
 - 4.2 Atidot..... 13
 - 4.3 MTR Labs..... 13
 - 4.4 A Regulator’s Perspective 13
 - 4.5 Getting Started on the Blockchain Journey 14
- Section 5: Acknowledgments 15**
- About The Society of Actuaries Research Institute 16**

Blockchain Opportunities for Insurance and Financial Industries

A workshop bringing together research and business applications

Executive Summary

Blockchain technology is rapidly evolving and gathering momentum within the financial industry. Many insurers and other financial institutions are taking interest in blockchain technology due to its potential to enhance operational and service infrastructure and processes. Adopting nascent digital technology can be daunting, but it is important for business leaders, including actuaries, to understand the new technology and its disruptive potential in the context of business applications.

On January 12, 2023, the Arizona Blockchain Applied Research Center (AZ BARC) and the SOA Research Institute jointly ran a workshop on the use of blockchain technology in insurance and financial industries. The workshop included presentations focused on academic research in the blockchain space by Arizona State University, AZ BARC and an industry expert panel assembled by the SOA Research Institute.

This document summarizes the research highlights and the discussions that occurred during the two-hour workshop. The topics included, but were not limited to, the following:

- Peer-to-peer insurance
- Modeling of smart contracts and other cyber risk losses
- Use of Zero Knowledge Proof in identity verification and decentralized data exchanges
- Blockchain-powered climate risk solutions
- Security solutions for blockchain risks

Section 1: Introduction

Arizona Blockchain Applied Research Center was founded in 2019 by the Partnership for Economic Innovation (PEI) with the aim to power industry with blockchain solutions. It consists of eight member companies: Intel, Early Warning, BD, Kudelski Security, Movemedical, MetaXFashion, DASH, and PEI. Each member of AZ BARC commits \$50,000 per year to join the center, and the private sector funding is matched for research projects by the State of Arizona. With nearly \$2 million in research project funding, the Center's research partner is Arizona State University. Members of AZ BARC have the right to commercialize the applications developed through research and, if no members decide to commercialize the application after one year, the applications will be made open-source to the public.

The topic of the workshop was blockchain opportunities for insurance and financial industries. The workshop featured presentations by Dr. Petar Jevtić and Dr. Dragan Boscovic from Arizona State University highlighting the past and current research projects at AZ BARC. The workshop ended with a panel discussion focused on business applications of blockchain technology.

Section 2: Blockchain Insurance Application and Blockchain Risks

In this section, Dr. Petar Jevtić discussed the research highlights of a peer-to-peer insurance project and a group of loss modeling projects in the intersection of blockchain and insurance: peer-to-peer insurance and the modeling of smart contracts and cyber risk losses.

2.1 PEER-TO-PEER INSURANCE

“Peer-to-Peer Insurance: Blockchain Implications”¹ was a research project funded by the SOA Research Institute and conducted by Arizona State University. The final report demonstrated an application of blockchain technology in the development of peer-to-peer (P2P) insurance.

P2P insurance is a business model where individuals or economic agents come together and pool their resources for mutual aid. Coupled with blockchain technology, this model allows for creating an insurance business that does not require centralized authorities and ensures an automated and trustworthy transaction environment. In the example, the researchers used Hyperledger Fabric technology, an enterprise grade distributed ledger that supports smart contracts. This report is a resource for insurers and reinsurers to get a taste of how to build blockchain-based insurance.

2.2 LOSS MODELING

A series of research works briefly presented fell within the scope of the multi-year research project, “Self-Adaptive Cyber Risk Management via Machine to Machine Economy Supported by Blockchain and Smart Contracts Technology.” The project was funded by the National Science Foundation (NSF) (Award number: 2000792) to advance cybersecurity of large-scale blockchain-enabled Internet of Things (IoT) systems via a novel organization of machine to machine economy². The relevant projects involved:

- Smart contract loss modeling: Smart contract risk can be defined as a financial risk of loss due to cyber attacks on or contagious failures of smart contracts. The research proposed a structural framework of aggregate loss distribution for smart contract risk under the assumption of a tree-stars graph topology representing the network of interactions among smart contracts and their users. The research provided analytical results and instructive numerical examples³.
- Cyber risk loss distribution of client-server networks: Across various businesses in different industries and sectors, a distinct pattern of IT network architectures, such as the client-server network architecture, may, in principle, expose those businesses, which share it, to similar cyber risks. Blockchain technology, including smart contracts, is abundantly used to solve various challenges in road traffic management and Vehicular Ad-hoc Networks. The research included a proposal of a structure framework for cyber risk in vehicle-to-vehicle cooperation for road space⁴.

¹ The full research report can be accessed at <https://www.soa.org/resources/research-reports/2021/p2p-insurance-blockchain/>.

² https://www.nsf.gov/awardsearch/showAward?AWD_ID=2000792

³ <https://doi.org/10.1142/S0219525921500144>

⁴ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4129369.

- Other related research works on cyber risk within the project scope include “Loss Distribution for Cyber Risk of Small and Medium-sized Enterprises for Tree-based LAN Topology⁵” and “Framework for Cyber Risk Loss Distribution of Hospital Infrastructure⁶”.

⁵ <https://doi.org/10.1016/j.insmatheco.2020.02.005>

⁶ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4063526

Section 3: Current Projects of Interest

In this section, Dr. Dragan Boscovic shared an overview of the current AZ BARC projects related to emerging blockchain technology. Furthermore, Zero Knowledge Proof and two of its applications, identity verification and decentralized data exchange, were discussed in depth.

3.1 CURRENT AZ BARC PROJECTS

Medical device inventory management

- Digital twins updates with blockchain technology were used to make sure there is a secure and valid data exchange between stakeholders (i.e., manufacturers, shippers and health providers).

Device ID management

- Monitor the state of operations and cyber risks on IoT devices using AI and machine learning. The blockchain is used as a data repository as well as to validate transitions of device states.

Intellectual property protection using NFTs

- Tokenization of fashion designs.

Multi-signature Analysis

- Analysis of cryptographic signing methods for transaction approvals.
- The objective is to analyze different options in terms of computational cost effectiveness.

Zero Knowledge Proof for KYC/AML

- Cryptographic method for concurrent identity verification and privacy protection.

Data exchanges for secondary datasets

- A marketplace for enabling metered use of relevant datasets by other interested parties while, at the same time, enabling privacy and copyright protection features of the leased datasets.

An abbreviated list of completed blockchain projects at ASU was also shared with the audience:

- Distributed Voting System - DAO centric voting system preserving voter confidentiality with verifiable tallying
- Peer-to-peer Microlending - Solution for real time auditing of small loans and charitable donations
- Blockchain Cybersecurity - Method to detect and analyze cybersecurity threats relative to Hyperledger Fabric operations
- Carbon Credit Tokenization - Automated accounting and real time auditing of corporate carbon social responsibility objectives
- Algorithmic Trading – AI-based algorithms for automated digital asset trading
- Velocity Protocol - Protocol for speeding up transaction synchronization and, consequently, scalability of blockchain applications

3.2 ZERO KNOWLEDGE PROOF AND ITS APPLICATIONS

Dr. Dragan Boscovic defined Zero Knowledge Proof (ZKP) as a way for one person to prove to another that he/she knows something without revealing what that something is. ZKP can also be applied to the context of machines. When exchanging information between two servers that are not owned by the same entities, ZKP can help validate that the information exchanged is properly acted on without having the identity of the machines involved.

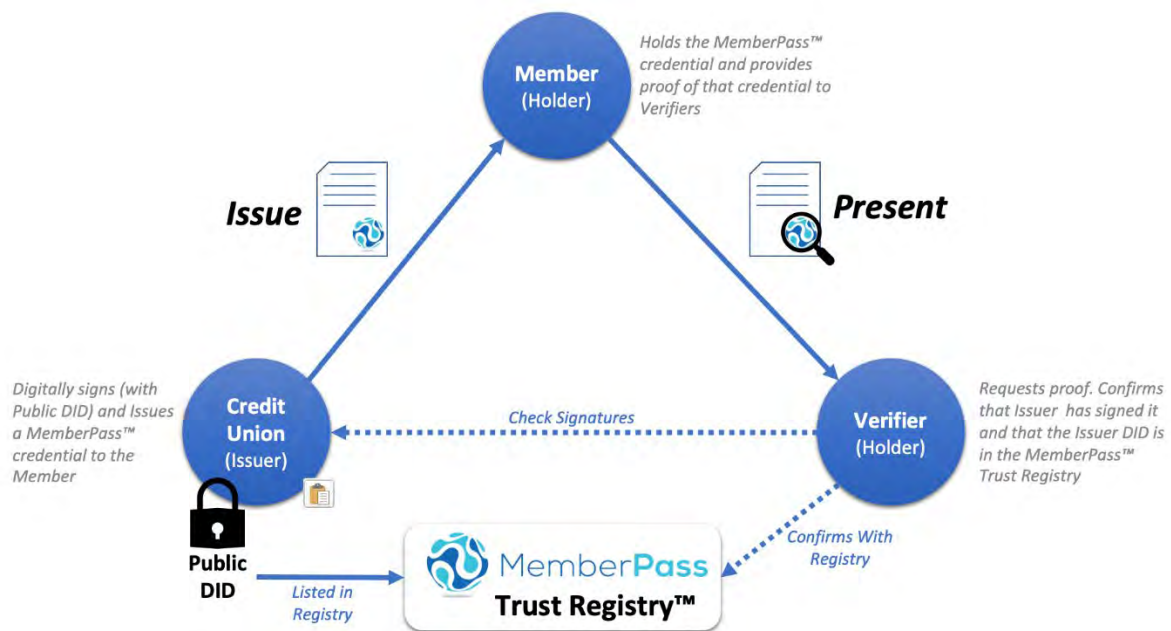
ZKP has a wide range of possible applications:

- Identity verification: prove that someone is who they claim to be without revealing any additional information (KYC and AML processes).
- Privacy-preserving protocols: perform a computation or exchange information without revealing any additional information to each other (online voting systems).
- Financial transactions: prove that someone has enough assets to make a certain financial transaction without revealing the exact amount of assets they possess.
- Verifying computational integrity: prove that a computation has been performed correctly without revealing the inputs or the computational steps used to arrive at the output.
- Data integrity: prove that data has not been tampered with without revealing the data itself.

Application 1 – ID Creation and Verification Workflow

Figure 1

ILLUSTRATION BY MEMBERPASS



A real application was built for a credit union in the United States. A customer with one bank needs to open an account with a different bank. When they go to the second bank, the same identity verification information would be asked of the customer, such as a driver's license and utility bills. These should be already known to the first bank the customer has an account with. The desire is to have a network of certifiers and verifiers, so consumers don't

have to provide the same information each time they start doing business with different organizations within the network.

The workflow of the identification network for a user, Alice, is as follows. First, Alice needs to download an app to register and enter all the information that is required for certifiers to validate her identity (e.g., upload a scan of her passport). The certifier will confirm the user’s identity and a unique ID will be issued and signed by the certifier with their private key. The ID, known as a Decentralized Identifier (DID), is a new type of identifier that enables verifiable, decentralized digital identification. Alice then accepts the verified claim, signs the claim with her user DID, and stores it in a private datastore of her wallet. When asked for identity information by another bank, Alice uses the app to grant access to the requested information for identity verification. The bank verifies signatures of the issuer DID and user DID to confirm Alice’s identity. The verification is complete without Alice needing to submit information twice.

The Proof of Concept has already been built and is using Hyperledger Indy technology. The professor welcomes interested partners to jointly build further applications.

Application 2 – Decentralized Data Exchange (DDEX)

Data is an increasingly valuable asset for businesses. Many companies and organizations generate private datasets, which are confidential and considered intellectual property with potential secondary applications. Kaggle.com, which allows users to find and publish datasets and build models with them, has demonstrated the value of data exchanges. To commercialize private data, a data exchange is needed where this private data can be sold to other private organizations or research labs.

A decentralized data exchange is not owned and operated by a specific legal entity. Rather, it is jointly operated by participants. The main benefit is that you can retain ownership and control of your own dataset while offering to share, which is not easily achievable by the centralized data exchanges. Some limitations of centralized data exchanges can be addressed by decentralized data exchanges as summarized below.

Table 1

DIFFERENCES BETWEEN CENTRALIZED AND DECENTRALIZED DATA EXCHANGES

Centralized Data Exchanges	Decentralized Data Exchanges
Excessive data storage and complexity in storing different types of data.	Decentralized data storage.
Centralized control by the storage solution provider.	Complete data ownership and control of the data.
Privacy concerns, especially when data is tabular and query-able.	No privacy issues.
Separate solution for managing access permissions and restrictions.	Simplified management of permissions and access through smart contracts.

Data exchanges face a unique challenge around retaining ownership of data. Imagine a scenario in which a user has been given the right to download a dataset from a decentralized data exchange. At that moment, the data owner loses control over his/her asset. If the data transmitted is in plaintext format, the data owner can’t be sure that the data has not be saved/copied/recorded in the original or other format (e.g., a screenshot). Both decentralized and centralized data exchanges have this limitation where it can’t prevent data from being copied once it has been

transferred or exposed to the buyer in plaintext format. Ideally, the data owner would grant the user the ability to use the dataset, execute their algorithms, get results, and verify the integrity of the datasets and the results. The data owner should be able to revoke the access of the data, and prevent the users from copying and using the data beyond the licensing agreement. AZ BARC has overcome this challenge by using Ocean Protocol, a marketplace to find, publish and trade datasets, where the user data is always kept on the premises.

AZ BARC is implementing two use cases of decentralized data exchanges:

Living Labs (crowd-sourced data collection): If a data user cannot find the data they need on an open exchange, they can commission a data-gathering campaign. The data buyer would provide the context of the data and the design for the experiments to be run by the data collector/seller. Payments (or other incentives) would be made once the integrity of the data is verified.

Compute data service: Providing the ability for researchers to execute their algorithms on the data owner's server or operational space and obtain results. The data owner will provide a verification of the execution of the algorithms and return only the results to the researchers. This way, the researchers can make use of relevant data, and the data owner retains the ownership of the data.

Proof of Concepts of these two use cases will be available in May 2023. The professor welcomed collaborations from data seekers and data owners.

Section 4: Panel Discussion

A panel discussion on insurance business applications of blockchain technology was moderated by David Schraub, Senior Research Actuary at the SOA. The panelists were:

- Mackenzie Mikkelsen, Chief Innovation Officer at Arbol
- Sreedhar Chintamaneni, Vice President of Business Development at Atidot
- Jimmy Yuen, Head of Product at MTR Labs
- Shane Foster, Deputy Director of the Arizona Department of Insurance and Financial Institutions

Each of the panelists provided an overview of their business and shared their thoughts on the future of applications of blockchain technology. Some panelists also shared their thoughts on how an insurance business could get started on their own blockchain journey.

4.1 ARBOL

Arbol is a climate risk solutions platform that helps businesses, often in agriculture or energy, mitigate climate risks related to perils such as rain, wind, sun, heat, freeze and storm. For example, many agriculture growers are interested in hedging their risk against rainfall. Arbol offers parametric and hybrid products via blockchain technology. Simply put, parametric contracts are contracts based on objective measures. For example, for every inch of rainfall below ten inches in January, the payout is \$10,000. The payout could vary from \$100,000 with no rainfall, or zero if there is ten inches or more of rainfall. In a parametric contract, a parametric trigger is defined based on a measurable data driven outcome, and a structure is also defined based on that.

The ecosystem built by Arbol is built to take advantage of decentralized technologies as much as possible. The evaluation of parametric triggers is done through a decentralized data platform hosted on the InterPlanetary File System (IPFS), a data file storage protocol that is immutable, distributed and permissionless. Arbol has built a parametric risk solution digital platform where clients can view data history and get a pricing quote from an artificial intelligence (AI) and machine learning (ML) powered underwriter for a hedge. Arbol uses a Chainlink node to connect the data platform on IPFS with their smart contracts to issue loss claim notices to insurers and reinsurers. Since the code is open source and the payout calculation is verifiable, Arbol has created a trustless environment for insurers and reinsurers to obtain the information they need.

Arbol has also created fully collateralized weather derivatives using smart contracts. When two parties, the insurer and the insured, enter into a smart contract ahead of the risk period, the data is automatically published to the data platform, and fed into the smart contracts via Chainlink oracle. At the end of the risk period, one can verify whether the parametric triggers have been met and issue a payout. More specifically, Arbol built a Chainlink adaptor that works with a partner company, dClimate network, to get the data to smart contracts. dClimate is responsible for gathering and hosting weather data and making it available.

The contracts can be issued on demand in the form of NFTs for a specific weather program. For all types of weather perils, once the templates have been established, smart contracts are scalable and can be used for NFT-based applications. They also developed a decentralized application to view the smart contract transactions, historical triggers and payouts that occurred.

Arbol has also been working on a hybrid product. Using their data platform to track storm data and model losses algorithmically using the storm data and a predetermined payout and exposure table, they can calculate the gross loss of the reinsurer based on a single weather event. Parametric insurance solutions are a great fit for blockchain use cases. They are highly data-driven and can leverage the immutability and trustlessness of blockchain.

4.2 ATIDOT

Atidot is an artificial intelligence company that makes predictions that are relevant to insurers and annuity companies. For example, Atidot uses data to predict lapses or customer churn over a predefined period of time. Such predictions are very valuable and actionable business intelligence. Similarly, they can also predict insurance customers' propensity to be upsold or cross-sold for targeted marketing.

The biggest restraint to doing more of this is lack of data and blockchain could solve this issue. Data is complicated. Because of the way data is captured and stored on the blockchain, the data on blockchain enables significant use cases for businesses. If a carrier's data is on the blockchain, a company like Atidot could run some models on the data. The carrier would have to grant data on the dataset and Atidot will be able to take that data and turn it into actionable intelligence in real time.

One use case that is going to be apparent is the ability to individually permit and monetize the access of the data. The insurance industry could be made more competitive due to the greater access to data and use of AI/ML technologies.

4.3 MTR LABS

MTR Labs is a DeFi incubator and the parent company that focuses on a suite of security related solutions that span decentralized finance (DeFi) and traditional finance. On the decentralized finance side, they are involved in InsurAce and Amulet protocols on Ethereum and Solana blockchains, respectively. There is a lack of security related solutions for the different projects that are being built on blockchains. Generally, engineers like to experiment and deliver products, but they could be doing it with less focus on safety. Teams at MTR Labs build safeguards and coverage for users who interact with smart contracts. They also partner with security audit firms and monitor the safety of smart contracts by assigning safety scores. Based on the security posture, insurance coverage can be provided through a peer-to-peer model. The current trend is that companies are increasingly catering to the digital world, or the metaverse, and smart contracts and blockchain usage will be part of it. There needs to be a lot more insurance applications around that specific field.

The panelist also shared a few thoughts around crypto in general. First, he debunked some crypto myths; for example, that crypto is exclusively for money launderers and smart contracts are bulletproof. He also shared his views on decentralized structures: Decentralized Autonomous Organizations (DAO) may not be the best structure for equal say and equal votes. The open nature of DeFi (OpenFi) is advantageous because being able to see transactions happen will minimize risks of fallouts and reduce the risks associated with the opaque nature of traditional organizations. He also shared that decentralized working groups on topics beyond blockchain are also thriving in the blockchain space, such as decentralized science and regenerative finance.

4.4 A REGULATOR'S PERSPECTIVE

The mission and goals of the regulators are to protect consumers, provide certainty to stakeholders and perform with efficiency and integrity as good stewards of taxpayer resources. It is important for regulators to be part of discussions about innovation and technology. Various committees have been formed, such as the technology, cybersecurity and innovation committee and the privacy committee, for regulators to discuss, monitor and better understand the blockchain space and develop policies to address emerging issues. If certain topics such as artificial intelligence touch other areas of concern, cross collaboration between committees could also happen.

From a regulator's perspective, it is important for businesses to understand their own project, implemented internally or provided by a vendor, and to be able to explain to a regulator how it works. If a business thinks there is vagueness or uncertainty in the law, the most efficient way to engage with a regulator is to do its due diligence and

arrive at a place where a regulator's input is needed, and then have a specific ask of what the business is looking for from the regulator, along with written documents articulating the business's opinions.

Also, consumer complaints are often a starting point for regulators to ask questions and figure out what went on. Depending on how the technology is utilized and comes into the regulated sphere, it needs to be looked at on a case-by-case basis.

One panelist also shared his view that there should be government action and oversight, but it is still early, and the development should not be restricted yet, as developers would use the best contract available to them regardless of geographical restrictions. An example of what he thinks the Web3 community would prefer is if some stolen funds off the blockchain were moved to a jurisdiction, the regulator of that jurisdiction would become aware and react accordingly.

4.5 GETTING STARTED ON THE BLOCKCHAIN JOURNEY

One question that the attendees were broadly interested in was how insurers and other financial institutions could get started on the blockchain journey if they only have very general knowledge of the blockchain.

One panelist said one can write parametric insurance on anything there is data for. It's important to focus on one's specialization to price risks appropriately. AI/ML techniques can be used to enhance competitive advantage. For a traditional insurer, a good starting point is to analyze an area they have a good understanding of and branch out there, including exploring hybrid programs which combine traditional and parametric insurance.

Another panelist said that it is hard to be in the state of utilizing all technological promise that is out there. Therefore, it is important to get started and keep moving where there is significant business value. Start with the technology that is available today and transition that technology to expand one's market and lower costs.

AZ BARC is already working on a number of applications that panelists mentioned, such as decentralized data exchanges, and has the capability to help businesses implement blockchain technology. AZ BARC welcomes participation and collaboration from the industry.



Give us your feedback!

Take a short survey on this report.

[Click Here](#)

SOA
Research
INSTITUTE

Section 5: Acknowledgments

The researchers' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the Project Oversight Group and others for their diligent work overseeing questionnaire development, analyzing and discussing respondent answers, and reviewing and editing this report for accuracy and relevance.

Project Oversight Group members:

Dragan Boscovic, Ph.D.

Petar Jevtic, Ph.D.

At the Society of Actuaries Research Institute:

David Schraub, FSA, MAAA, Senior Practice Research Actuary

About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its [strategic research programs](#): aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of [topical research available](#), including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute
475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
www.SOA.org