Blockchain Opportunities for Insurance and Financial Industries

ARIZONA BLOCKCHAIN APPLIED RESEARCH CENTER

David Schraub, Shane Foster, Sreedhar Chintamaneni, Mackenzie Mikkelsen, Jimmy Yuen

Thursday, January 12th – 2:00- 4:00 PM

SOCIETY OF ACTUARIES®

Agenda

SOCIETY OF ACTUARIES®

Agenda

I. Intro BARC / setting objectives for the workshop — 2 min

II. Insurable Blockchain Risks / 2 examples Dr Jevtic (ASU/ Math School) — 20 min

Smart Contracts Risk Modelling
M2M economy

III. Current BARC projects of interest Dr Boscovic (ASU/SCAI) — 20 min

Secondary Data Market Place
ZKP - KYC application

IV. Panel Session: Business Applications — 60 min

David Schraub, SOA, moderator, dschraub@soa.org, Actuarial Association
Arbol, Mackenzie Mikkelsen, mackenzie@arbol.io, Parametric insurance
Atidot, Sreedhar Chintamaneni, sreedhar@atidot.com, AI solution provider
MTR Labs, Jimmy Yuen, jimmy@mtrlabs.com, DeFi Incubator
Shane Foster, DIFI, Regulator

Description: Each panelist will present a brief overview of existing technologies they see available for AZ carriers to help innovate further in their business.

V. Q&A — 18 min

School of Mathematical and Statistical Sciences

Petar Jevtic

Assistant Professor

ASU
ARIZONA STATE UNIVERSITY

Outline

- My background
- Two projects that started the journey with the Blockchain Lab (one funded by SOA!)
- Other NSF funded projects…

School of Mathematical and Statistical Sciences
Arizona State University

Background - Petar Jevtic

- **Educational Background**
  - **Ph.D. Economics** - Statistics and Applied Mathematics, University of Turin, Italy

    (Visiting Scholar: Statistics Department, The Wharton School, UPenn)
  - **M.S. Economics** - Faculty of Economics, University of Belgrade, Serbia
  - **Dipl. Ing. Computer Science and Engineering** - University of Belgrade, School of Electrical Engineering, Serbia
- **Academic Professional Background**
  - **Assistant Professor** - **Actuarial Science** - Arizona State University, USA (Aug 2017 -)
  - **Assistant Professor** - **Math. Fin. and Actuarial Science** - McMaster University, Canada (Jul 2014 - Jul 2017)
  - **Postdoctoral Fellow** - **Math. Fin.** - McMaster University, Canada (Sep 2013 - Jun 2014)
- **Research Interests** - Vision: "Create practical and robust mathematical models of risk."
  - **Methodological**: Predictive Analytics, Applied and Theoretical Probability, Spatial Analysis, Stochastic processes and geometry (Lévy Processes, Marked Point Processes, Random Graph Theory, Spatial Point Processes)
  - **Domain**: P&C, Cyber risk, Smart contract risk, Smart Cities, Telematic data, Autonomous Systems, Longevity Risk, Pension Mathematics, Health Insurance (Wearable tech), Mathematical Finance
- **Research group** (currently: 4 PhD students)
- **Global network of co-authors**

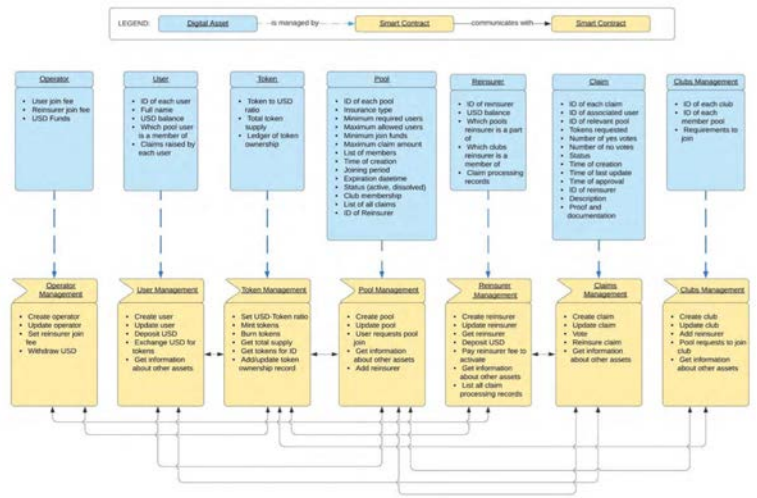
ASU School of Mathematical and Statistical Sciences
Arizona State University

Project – *Peer-to-Peer Insurance: Blockchain Implications*

- Motivation: *"Peer-to-peer (P2P) insurance, a business model where individuals or economic agents join together and pool their resources for mutual aid. Coupled with blockchain technology, this model allows for creating a business that does not require centralized authorities and ensures an automated and trustworthy transaction environment.."*
- *Project goal: In the context of enterprise grade Hyperledger Fabric technology we develop an example of P2P insurance application. "Step by step, we show how a traditional insurer could be part of the development…"*
- *Project result: "we showcase the development of a P2P insurance model and analyze it from a technological and product perspective."*
- *Output: First of its kind report for SOA.*

https://www.soa.org/globalassets/assets/files/resources/research-report/2021/p2p-insurance-blockchain.pdf

Figure 7
ASSETS OF THE BLOCKCHAIN NETWORK AND THEIR RESPECTIVE SMART CONTRACTS



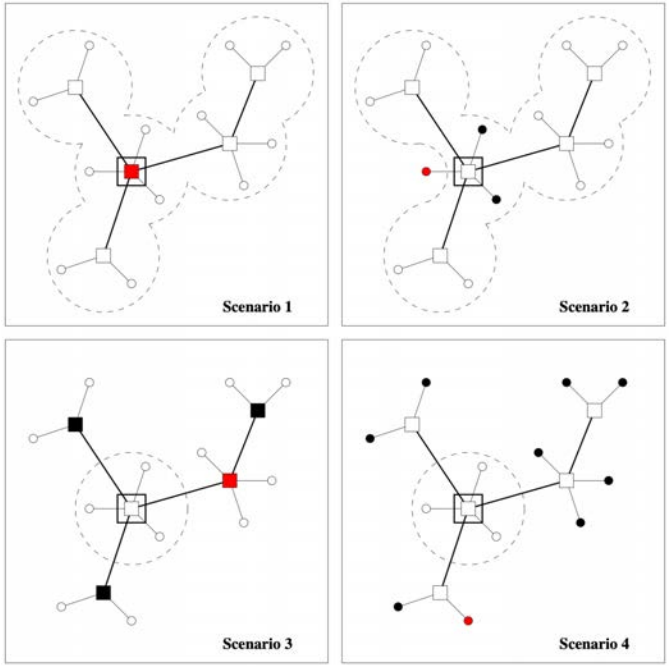
Source: Report linked below.

School of Mathematical and Statistical Sciences
Arizona State University

SOA FUNDED PROJECT!

Project – *Smart Contracts Loss Modeling*

- Motivation: *"Smart contract risk can be defined as a financial risk of loss due to cyber attacks on or contagious failures of smart contracts."*
- *Project goal: Create "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."*
- *Project result: Analytical characterization of mean and variance of loss distributions.*
- *Output: First of its kind in the academic literature.*



Source: The paper referenced below.

Advances in Complex Systems | VOL. 24, NO. 07n08

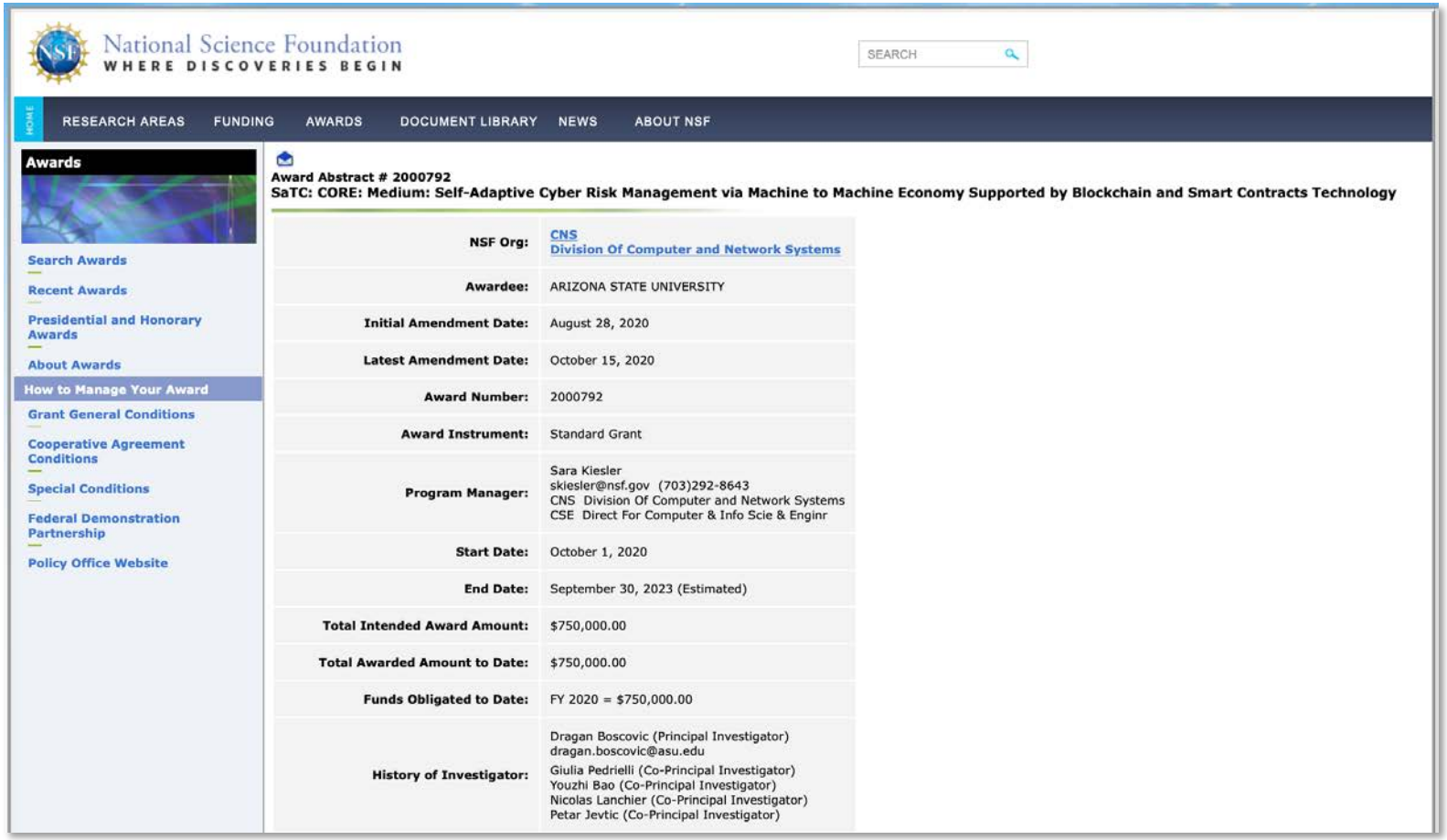
PROBABILISTIC FRAMEWORK FOR LOSS DISTRIBUTION OF SMART CONTRACT RISK

PETAR JEVTIĆ and NICOLAS LANCHIER

https://doi.org/10.1142/S0219525921500144

School of Mathematical and Statistical Sciences
Arizona State University

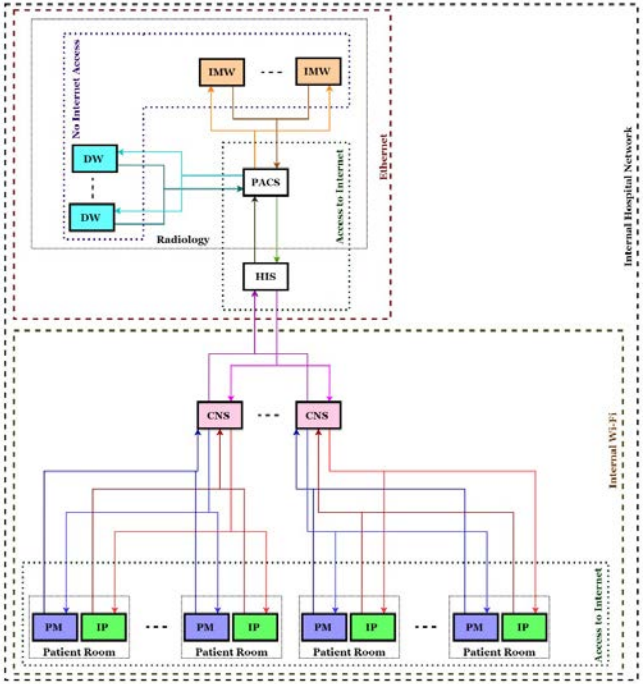
NSF **FUNDED PROJECT!**



Source: Screenshot from: https://www.nsf.gov/awardsearch/showAward?AWD_ID=2000792

Project – *Loss Distribution of Hospital Infrastructure*

- Motivation: *"Networks like those of healthcare infrastructure have been a primary target of cyberattacks for over a decade. From just a single cyberattack, a healthcare facility would expect to see millions of dollars in losses from legal fines, business interruption, and malpractice lawsuits. As more medical devices become interconnected, more cyber vulnerabilities emerge resulting in more potential exploitations that may disrupt patient care and result in catastrophic financial losses."*
- *Project goal: For various types of losses, characterize the of cyber risk loss distribution of a hospital infrastructure. Account for various IOT devices such infusion pumps, patient monitors, nursing stations, imaging devices…*
- *Project result: Analytical characterization of mean and variance of various aspects of loss distributions.*
- *Output: Academic paper in advance stage of review for Risk Analysis Journal.*



Source: The paper referenced below.

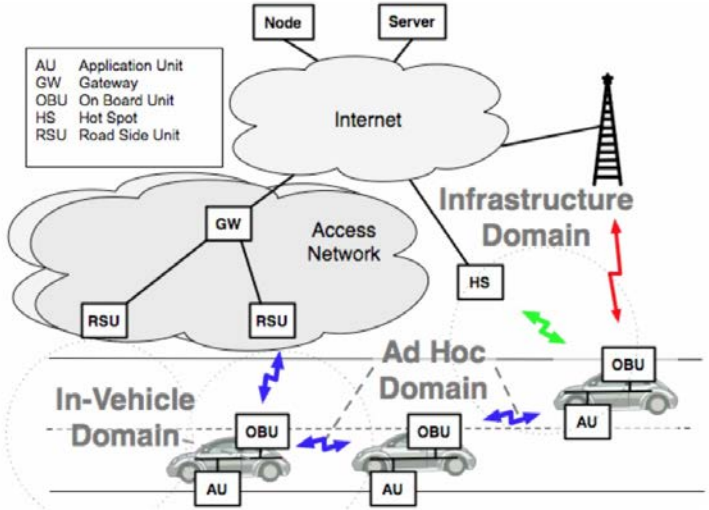
School of Mathematical and Statistical Sciences
Arizona State University

NSF **FUNDED PROJECT!**

Chiaradonna, Stefano, Petar Jevtic, and Nicolas Lanchier. "Framework for Cyber Risk Loss Distribution of Hospital Infrastructure: Bond Percolation on Mixed Random Graphs Approach." Available at SSRN 4063526 (2022).

Project – *Framework for Cyber Risk Loss Distribution of Client-Server Networks*

- Motivation: *"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.*
- *Project goal: "propose a probabilistic structural framework for loss assessments of cyber risks on the class of client- server network architectures with K different client types."*
- *Project result: The results are corresponding exact means and variances of cyber risk loss distributions. Example of use cases: implantable medical devices in healthcare, smart buildings infrastructure, application for ride-sharing services such as Uber and Lyft, and application of vehicle-to-vehicle cooperation in traffic management.*
- *Output: First of its kind paper submitted to Annals of Operations Research Journal.*



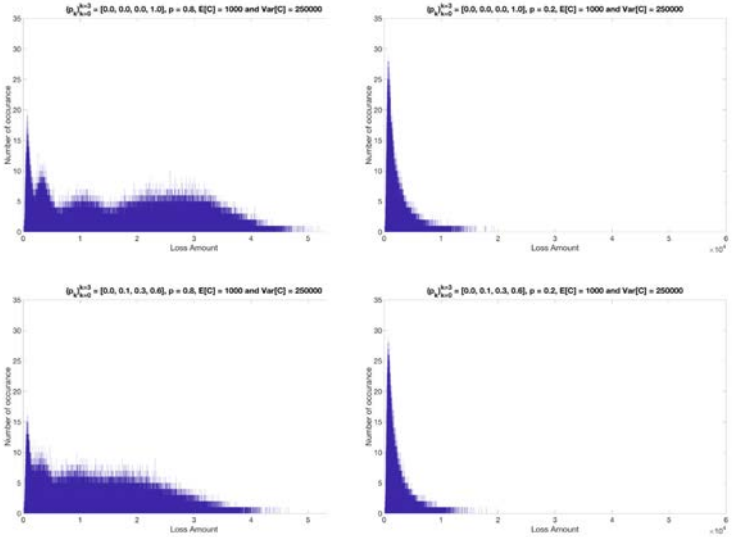
Source: Car 2 Car Communications Consortium Manifesto.

School of Mathematical and Statistical Sciences
Arizona State University

NSF **FUNDED PROJECT!**

Chiaradonna, Stefano, et al. "Framework for Cyber Risk Loss Distribution of Client-Server Networks: A Bond Percolation Model and Industry Specific Case Studies." *Available at SSRN 4129369* (2022).

Project – *Loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology*



Source: The paper referenced below.

- Motivation: Cyber risk implications of small and medium-sized companies might have grave implications for companies themselves as well as insurers. However, that risk can be gauged, especially since IT networks across these companies might have shared characteristics of LAN.
- *Project goal: develop "structural model of aggregate loss distribution for cyber risk of small and medium-sized enterprises under the assumption of a tree-based LAN topology."*
- *Project result: Parametrized characterization of aspects of loss distribution, for various sizes of IT network.*
- *Output: A paper published in a premier insurance journal!*

School of Mathematical and Statistical Sciences
Arizona State University

Jevtić, Petar, and Nicolas Lanchier. "Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology." Insurance: Mathematics and Economics 91 (2020): 209-223.

Thank you for your attention!

if you want to reach out, please feel free to contact me on

petar.jevtic@asu.edu

School of Mathematical and Statistical Sciences
Arizona State University

Ira A. Fulton Schools of Engineering

Arizona State University

Blockchain Research Lab

Current AzBARC Projects

Dr. Dragan Boscovic

About me

Dragan Boscovic, PhD in computational electromagnetics.
Bath University, UK
http://www.google.com/#q=dragan+boscovic

19 years at Motorola Labs (building and creating advanced technology organizations)

- 1991-1997 Basingstoke, UK
- 1997 - 2004 Paris, France
- 2004 -2008 Chicago, US
- 2008 - 2010 Beijing, China

2 years at Google, 3 years at Stanford and 6 years at ASU

ASU:

- **Research Professor**
- **Director, Blockchain Research Lab**
- **Technical Director, Center for Data Engineering**
- **Research Director, AZ Blockckchain Applied Research Center**

BARC Projects

Medical Device Inventory Management

- Digital Twins updates by Device Manufacturer, Shipper and Health Provider

Device ID Management

- IoT Cybersecurity application based on digital threading and ML/AI analysis

Zero Knowledge Proof for KYC/AML

- Cryptographic method for concurrent identity verification and privacy protection

Intellectual Property protection using NFTs

- Tokenization of fashion designs and fusion between DEX and physical sales

Multisignature Analysis

- Analysis of different cryptographic methods for multisignature Tx approvals

Data Exchanges for Secondary Data sets

- A Market-Place for selling and buying private data sets

ASU Blockchain Research Projects (abbreviated list)

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 analyse 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 Tx synchronization and consequently scalability of blockchain applications

ZKP - Zero Knowledge Proof

What is ZKP

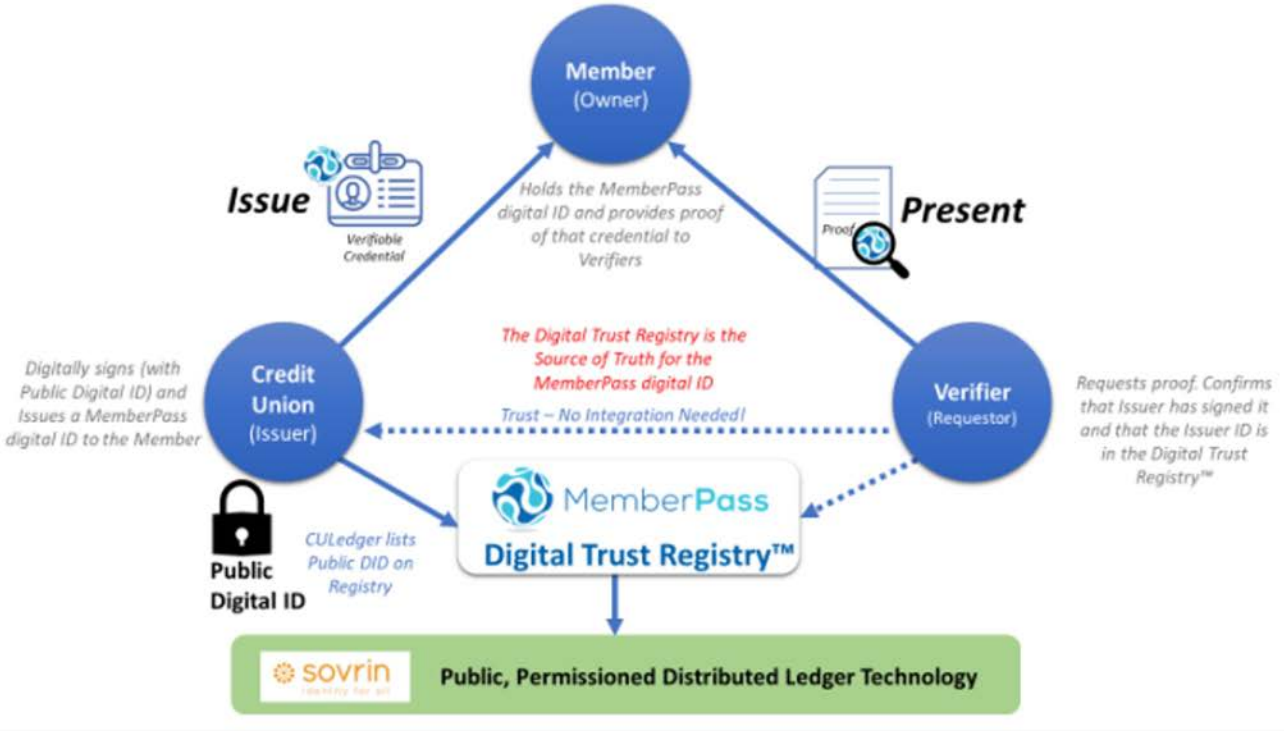
General Definition:

- A zero-knowledge proof (ZKP) is **a way for one person to prove to another that he/she knows something, without revealing what that something is.**

Examples of possible applications:

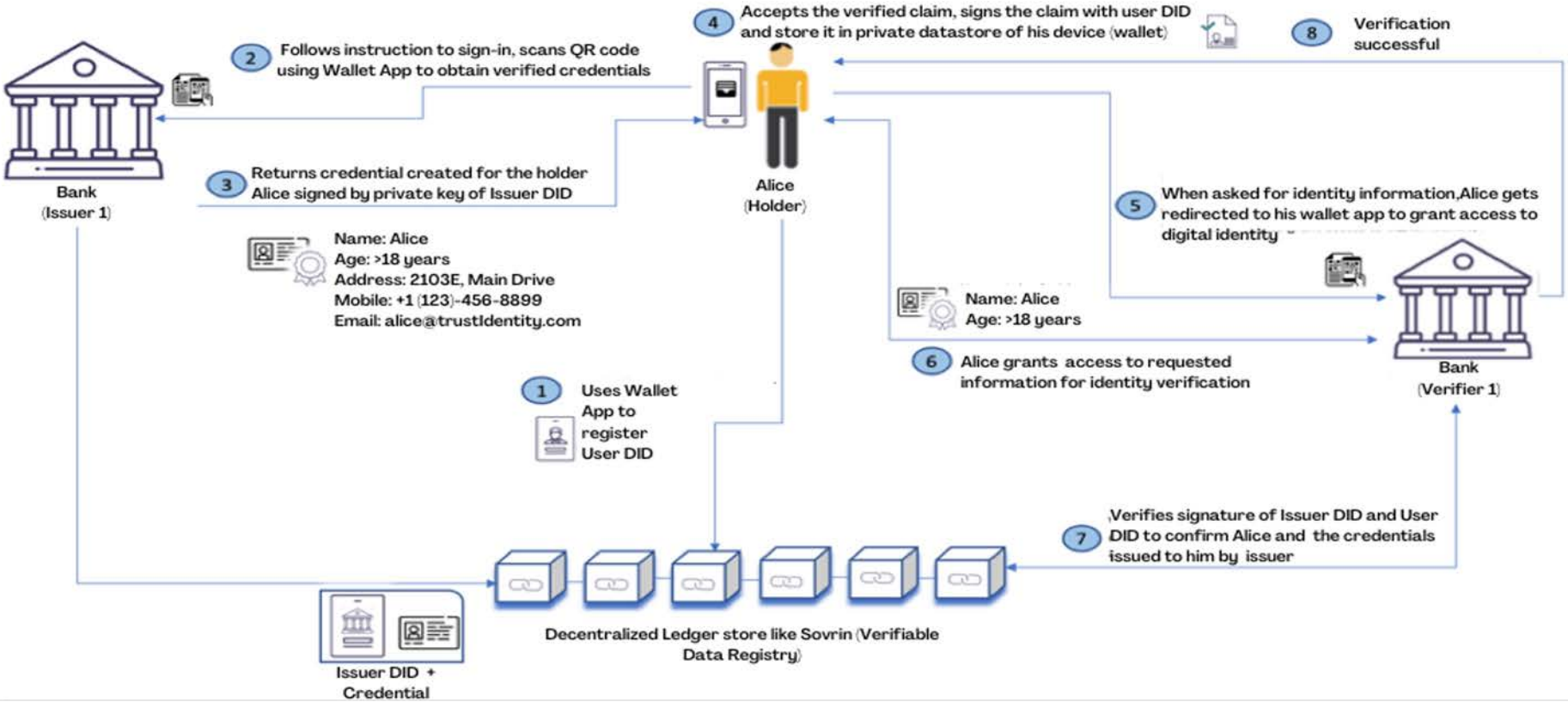
- *Identity verification*: prove that someone is who they claim to be, without revealing any additional information
- *Privacy-preserving protocols*: perform a computation or exchange information, without revealing any additional information to each other (online voting systems).
- *Financial transactions*: 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.

Identity Verification



Above picture is taken from MemberPass

How it works: ID creation and verification workflow



Current Platform: Call for Application/Trial Partners

What is Zero-Knowledge Proof (ZKP)?

A zero-knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that they know a certain piece of information, without revealing what that information is.

PoC is using Hyperledger Indy technology

This is a **call for interested partners to jointly build a specific application/use case** on top of the PoC developed.

DDEX Decentralized Data Exchange

Why do we need a DEX?

- Kaggle.com is great resource and the DEX need validator
  - all the code & data you need to do your data science work with over 50,000 public datasets and 400,000 public notebooks
- Many companies/organization generate private datasets which are confidential and considered as IP, with potentially secondary applications.
- To commercialize private data we need a data exchange where this private data can be sold to other private organizations or research labs.

Centralized DEX vs Decentralized DEX (CDEX vs DDEX)

There are few limitations with centralized data exchanges

- Excessive data storage and complexity in storing different types data.
- Centralized control by the storage solution provider.
- Privacy concerns especially when data is tabular and queryable
- Separate solution for managing access permissions and restrictions

Decentralized DEX has certain advantages over centralized DEX

- Decentralized data storage
- Complete data ownership and control of the data
- No privacy issues
- Simplified management of permissions and access through blockchain smart contracts

DEX Challenge

- **Imagine a scenario** in which a user has been given the right to download a dataset from DEX.
- At that moment, the data (IP) owner loses control over his/her asset!
- If data transmitted is in plaintext format, we can't be sure that the data has not be saved/copied/recorded in original or another format (screenshot).
- **B**oth decentralized or centralized DEX have this limitation that it can't prevent data from being copied once it has been transferred or exposed to the buyer in plaintext format.
- *We overcome this challenge by using Ocean Protocol where we always keep the user data on premise.*

Implementing two DDEX use cases

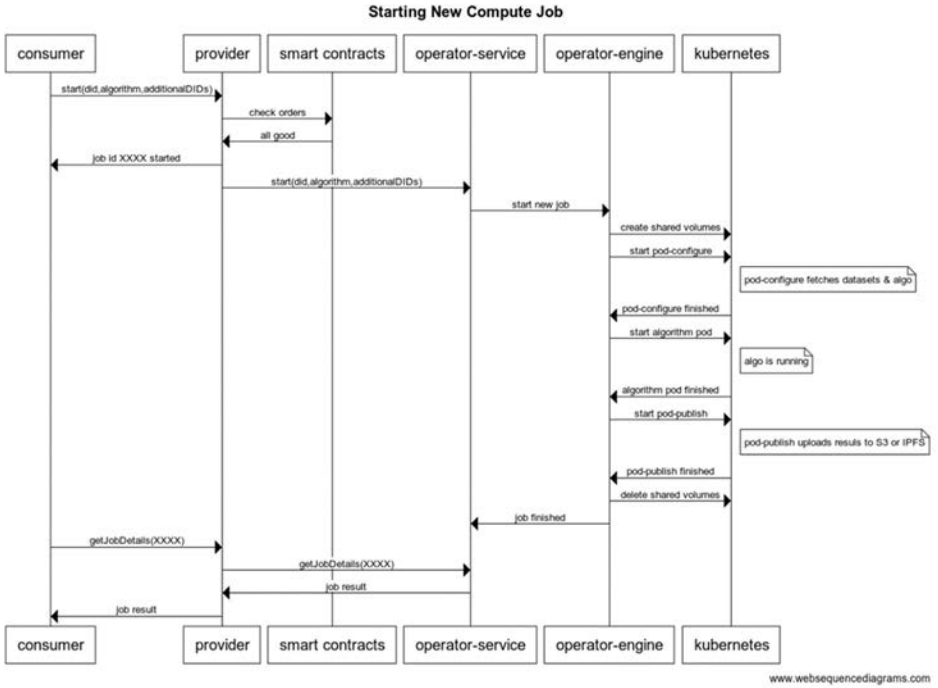
Living Labs:

- Data buyer can commission data gathering campaign by providing design for the “experiments” run by the data collector/seller
- Buyer has ability to check compliance of the data against the experiment design

Compute Data Service:

- Customer algorithm is working with data on the seller side and returns the results
- Buyer can check the integrity of data set by running its “data” QC algorithms

PoC available May 2023



Ira A. Fulton Schools of Engineering

Arizona State University

Blockchain Research Lab

Thank you!

SOCIETY OF ACTUARIES
Antitrust Notice for Meetings

Active participation in the Society of Actuaries is an important aspect of membership. However, any Society activity that arguably could be perceived as a restraint of trade exposes the SOA and its members to antitrust risk.

Accordingly, meeting participants should refrain from any discussion which may provide the basis for an inference that they agreed to take any action relating to prices, services, production, allocation of markets or any other matter having a market effect. These discussions should be avoided both at official SOA meetings and informal gatherings and activities. In addition, meeting participants should be sensitive to other matters that may raise particular antitrust concern: membership restrictions, codes of ethics or other forms of self-regulation, product standardization or certification. The following are guidelines that should be followed at all SOA meetings, informal gatherings and activities:

- DON'T discuss your own, your firm's, or others' prices or fees for service, or anything that might affect prices or fees, such as costs, discounts, terms of sale, or profit margins.
- DON'T stay at a meeting where any such price talk occurs.
- DON'T make public announcements or statements about your own or your firm's prices or fees, or those of competitors, at any SOA meeting or activity.
- DON'T talk about what other entities or their members or employees plan to do in particular geographic or product markets or with particular customers.
- DON'T speak or act on behalf of the SOA or any of its committees unless specifically authorized to do so.
- DO alert SOA staff or legal counsel about any concerns regarding proposed statements to be made by the association on behalf of a committee or section.
- DO consult with your own legal counsel or the SOA before raising any matter or making any statement that you think may involve competitively sensitive information.
- DO be alert to improper activities, and don't participate if you think something is improper. If you have specific questions, seek guidance from your own legal counsel or from the SOA's Executive Director or legal counsel.

SOCIETY OF ACTUARIES

Presentation Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the participants individually and, unless expressly stated to the contrary, are not the opinion or position of the Society of Actuaries, its cosponsors or its committees. The Society of Actuaries does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented. Attendees should note that the sessions are audio-recorded and may be published in various media, including print, audio and video formats without further notice.

Bios

SOCIETY OF ACTUARIES®

David Schraub

David Schraub is Senior Practice Research Actuary, responsible for the Actuarial Innovation and Technology strategic research program as well as the InsurTech initiative.

David is an FSA, CERA, MAAA, AQ

dschraub@soa.org

Mackenzie Mikkelsen

Mackenzie is the current Chief Innovation Officer of Arbol. There, his directive is to push the web3 frontier of the insurance industry by expanding Arbol's capabilities with the blockchain and smart contracts. His background is in engineering and finance. At Arbol, he explores ways that the latest advancements in DeFi can be leveraged to bring improvements to insurance practices.

mackenzie@arbol.io

Sreedhar Chintamaneni

Sreedhar has over 20 years of corporate finance and investment experience. He joined Atidot after spending years at Guardian Life as a VP Strategy and, previously, a senior vice president of Deutsche Bank. He has closed over 150 corporate transactions, including venture capital and private equity investments, debt and equity financing, and mergers and acquisitions.

sreedhar@atidot.com

Jimmy Yuen

Jimmy Yuen leads product development and strategy at MTR Labs – a DeFi incubator. He is a credentialed actuary (FSA, FCIA) and former consultant at Willis Towers Watson focused on developing investment strategies for $10B+ of Canadian pension assets including the growth of the outsourced CIO business.

He joined the team in 2021, having invested in the digital assets space since 2017.

jimmy@mtrlabs.com

Shane Foster

Deputy Director Shane Foster joined the Arizona Department of Insurance and Financial Institutions ("DIFI") in November 2020. Before joining DIFI, he served as Senior Litigation Counsel in the Consumer Protection & Advocacy Section of the Arizona Attorney General's Office. In this role, Mr. Foster participated in several high-profile matters, including Arizona's consumer fraud lawsuits against JUUL, Eonsmoke, CashCall, and Mercedes-Benz, handled data privacy matters, and played a significant role in the administration of Arizona's Fintech Sandbox. Prior to being promoted to Senior Litigation Counsel, he served as an Assistant Attorney General in the State Government Division.

Deputy Director Foster began his legal career as a transactional attorney in New York and has extensive experience in the mortgage industry. Deputy Director Foster earned a B.A. from Brigham Young University and a J.D. from Cornell Law School.

Polling questions

SOCIETY OF ACTUARIES®

Question #1

What lines of business do your company carry?

[choose all that apply]

- P&C Personal lines
- P&C Commercial lines
- Life & Annuity
- Health
- Financial institutions with deposits (e.g. retail bank)
- Financial institutions without deposits (e.g. pension funds)
- Others [please use the chat function]

Question #2

What technologies you are most interested in?

[please answer using the chat function]

Question #3

How far along are you in your journey for the most advanced project?

[choose one]

- General Education
- Need assessment, scoping
- RFP
- POC
- Partnership
- Refinement and iteration

Question #4

What is your largest obstacle?

[please answer using the chat function]

Question #5

What is your level of technical knowledge?

[choose one]

- Beginner – Attended a few presentations on the topic
- Initial step – Understand general concepts
- Aware – Understand what you know and what you don’t know
- Advanced – Able to articulate technical questions
- Expert – Able to answer technical questions

SOA

SOCIETY OF ACTUARIES®

SOA InsurTech

Always looking for ways to provide content

- Office Hours
  - InsurTech can pick the brain of an actuary for a few hours
- Networking at InsurTech event
  - ITC, InsurTech NY, Insight Insurtech…
- Podcast
- Mentoring and Job posting
- Research

SOA Research

Any topic suggestions for the next research?

- Decentralized Finance for Actuaries
- Peer-to-Peer Insurance: Blockchain Implications
- Avoiding Unfair Bias in Insurance Applications of AI Models
- Fostering Innovation: A Guide for the Actuarial Industry
- Decentralized Insurance Alternatives: Market Landscape, Opportunities, and Challenges
- A Risk Classification Framework for Decentralized Finance Protocols
- Actuarial Technology Issues - A Roundtable Discussion - August 2022 Update

Arbol

SOCIETY OF ACTUARIES®

Arbol - Innovations

- Parametric and hybrid products for climate related perils- Rain, Wind, Sun, Heat, Freeze, Storm
- Decentralized data platform on IPFS - Immutable, Permissionless, Distributed
- Abol Chainlink Node- Decentralized data model for delivering claims/payout calculations to smart contracts

Arbol - Blockchain Use Cases

- Fully collateralized weather derivative smart contract
- NFT-based reinsurance application
- Wind Catastrophe insurance/reinsurance program


SOCIETY OF
ACTUARIES®