**BLOCKCHAIN AND AI ALGORITHMS FOR DISASTER RESPONSE**

**STUDENTS:** MILAD FOTOUHI, JIARONG QIAN, NANSHUN YUAN

---

**Implementation: Blockchain for Private Information Sharing**

- Those affected by a disaster may not wish to provide access to their belongings and share more information than necessary.
- We propose a solution by using smart contracts imbedded in each block of a blockchain.
- As a simple, practical, and efficient mechanism, our algorithm uses a single trusted blockchain to support a large number of side blockchains, with low computational cost.

**Implementation: Using Ethereum as a Secure Mechanism to Store Data**

- Ethereum has demonstrated itself to be secure in practice but at the expense of poor performance.
- We have decided to implement an out-designed smart contract into Ethereum in order to have a high performance blockchain without sacrificing security.
- We propose an intermediate “data availability oracle” layer that interfaces between the side blockchains and the trusted blockchain. This oracle layer accepts blocks form side blockchains and pushes verifiable commitments to the trusted blockchain.

**Implementation: Conditional Secret Sharing On Ethereum**

- Conditional secret sharing should be implemented so that the secret on the blockchain will be revealed in a disaster only if the majority of secret shareholders wish to reveal the secret.
- An attacker with unlimited computational power should not be able to break the decrypted share to access the data without having enough shares to meet the threshold, or minimum number of shares.
- The implementation should be simple and efficient.

---

**Motivation**

In the immediate aftermath of a mega-quake, all disaster response agencies and personnel will be completely overwhelmed. External help (primarily from the government) is unlikely to come immediately after a disaster. If neighborhoods rely mostly on such help as the status quo is now, it is likely there will be more fatalities and greater economic loss. As a result, neighborhoods are urged to prepare for community-based survival for up to three weeks. This means that residents must be able to share useful information, carry out essential activities (e.g., staying cool/warm in summer/winter, securing food), and use effective socially-integrated technological solutions to enhance their ability for survival and real-time response. In this project, we develop technologies that enable real-time information gathering and sharing (while safeguarding privacy), and solutions for efficient resource matching by leveraging social ties. These include:

- Technologies that both enable and implement near real-time or best effort information gathering.
- Decentralized solutions for storage and sharing of the information.
- Privacy-preserving methodologies to protect sensitive user data.

---

**Results**

- We have achieved an average accuracy of 96% on UKIMI’s and 91% on NSCLab with 5 fold cross validation.

**Future Work and Reference**

As we've finished our Oracle layer, blockchains, and implementation of Shamir secret sharing, we've begun integrating Shamir secret sharing with our blockchain structure. For future work, we would be testing the integrated system, perfect our AI text mining system, and design a front-end app that allows users to easily utilize our application.