BLOCKCHAIN AND AI ALGORITHMS FOR DISASTER RESPONSE

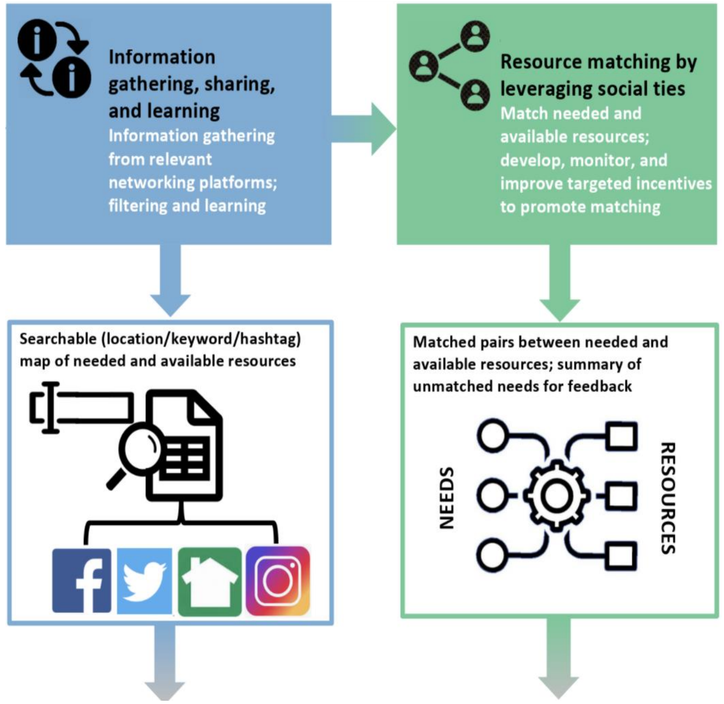
STUDENTS: MILAD FOTOUHI, JIARONG QIAN, NANSHUN YUAN

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.

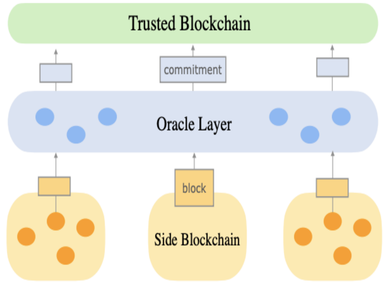
Requirements: Prototype Elements



- A privacy-aware document showing goods/services needed/anticipated and available/ anticipated, generated form AI data mining.
- A framework for information dissemination that can leverage the wealth of information from user profiles as well as user interactions on community forums (ex, nextdoor app).

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.



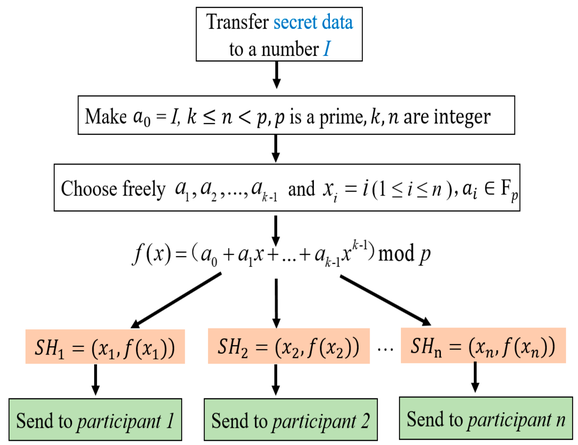
Implementation: Using Ethereum as a Secure Mechanism to Store Data

- 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

Requirements

- 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.



Progress to Date

- A private information sharing method has been developed based on Shamir secret sharing.
- We have incorporated Shamir secret sharing method into a multi-signature smart contract scheme to achieve our desired conditional secret sharing mechanism.

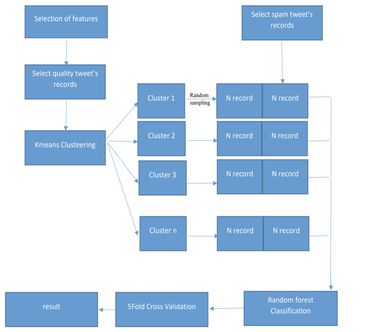
Implementation: AI for Text Mining During a Disaster

- While textual information is abundant in public forums, there exists the problem of misinformation. We have developed a robust aggregation method that incorporates multiple sources of information while ensuring noises can be filtered out.
- We have extracted suitable features based on previous results. We have started to build prediction models by adding features one by one and checking the result.
- For the evaluation of our solution we used 2 datasets. The first one is UtkMl's1 twitter dataset and the second is a much larger imbalanced dataset from NSCLab.

Results

- We have achieved an average accuracy of 96% on UtkMl's1, and 91% on NSCLab with 5 fold cross validation.

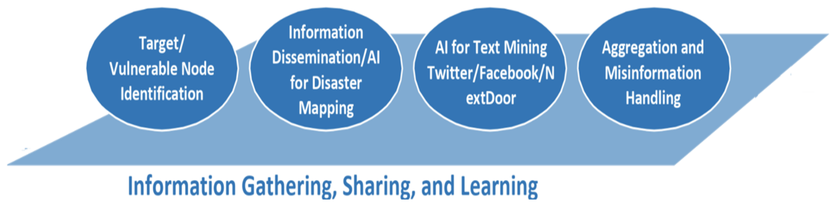
Feature	description
Tweet	This is the text that was tweeted
following	The number of people the account that tweeted is following
followers	The number of people following the account that tweeted
actions	The total number of favorites, replies, and retweets of said tweet
is_retweet	Binary [0,1] value: If 0 its not a retweet, if 1 it is a retweet
location	The self-written location provided by the user on their profile, May not exist, be "Unkown", and is NOT standardized! ex. could be ("NY", "New York", "Upper East Side", Etc!)
Type	Either Quality or Spam



Implements: AI to Generate Source Map of Disaster

Approach

- Developing robust aggregation methods that incorporate multiple sources of information while ensuring that noises can be filtered out.
- Designing a framework for text mining that will extract information from multiple forums about individuals in need as well as generate a community source map of disaster. Leverage AI to create such a map.
- Besides densely populated urban areas, we will also consider sparsely populated areas where social network updates may be infrequent and need to be combined with other remote sensing type data to provide meaningful analytics.



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.

1. Shamir, Adi. "How to share a secret." *Communications of the ACM,* 22.11 (1979): 612-613.
2. Sheng, Pejyao. et al. "ACeD: Scalable Data Availability Oracle. " arXiv:2011.00102(2020).
3. http://nsclab.org/nsclab/resources/ | https://www.kaggle.com/c/twitter-spam/overview

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON

ADVISORS: SREERAM KANNAN, PAYMAN ARABSHAHI, WEI CHENG
SPONSORS: NATIONAL SCIENCE FOUNDATION,
ELECTRICAL & COMPUTER ENGINEERING DEPARTMENT, UNIVERSITY OF WASHINGTON