HealthChain: Rapidly Providing Medical Data to Emergency Medical Responders

We are HealthChain:

We are using blockchain technology to provide medical data in times of emergency. Our technical solution has three components: taking a biological key from a victim and extracting a unique, reproducible key that we then pass into blockchain, where we store the functions that locate and retrieve their emergency medical record from an IPFS infrastructure. Finally, we serve that record to EMTs seamlessly in their emergency first response standard operating procedure workflow.

Problem and Proposal

The third leading cause of death in the United States is medical error. When Emergency First Responders don't have access to the full information of a victim's underlying medical conditions, they can make errors in treatment in the first crucial moments of their medical response that can change the patient's outcome. Because patients are often unconscious or unreliable, getting the right data at the right time is a major bottleneck in the emergency first response.

HealthChain eliminates this bottleneck by using a biological key that can be extracted from the victim to verify their identity and authenticate access to their medical information. Blockchain and IPFS allow for a decentralized, public, but secure system to shield the privacy of the victim's medical record. Finally, serving this record to EMTs seamlessly saves them precious time and helps guide their course of treatment so they can focus on their priority of saving the victim's life.

To solve this we started by breaking our team into three groups - one to focus on each component of our technical solution: Biological Authentication and the data science pipeline to extract a key from a biological element, Blockchain, and the real world deployment of such a tool. We originally started working with iris scans, because we learned that irises are sufficiently unique. We began doing data processing on iris scans and acquiring a dataset, while the deployment team established a connection with the San Francisco Fire Department, and two team members spent a day shadowing Emergency First Responders. We learned that in fact an iris would not work as a biological key for a few reasons: first, when someone is in pain they clench their eyes. Second, often victims are combative or in an altered mental state, and make it very difficult to get near their face - often this is so extreme EMTs have to place a mesh "spit sock" on the patients head and use restraints to protect themselves. Third, eyes are so delicate that trying to force compliance could result in unintentional injury to the patient. However, we noticed that standard operating procedure for EMTs was to use a pulse oximeter to take the victim's pulse oxygen level as one vital sign to monitor the patient's condition. This pulse oximeter is a gentle clip that is placed around the patient's finger. We also learned that there is precedent in San Francisco that in order to register for social services, at the point of registration they take a photograph and a fingerprint to identify individuals. The fact that we would not have to ask EMTs to change their standard operating procedure by integrating a fingerprint scan into the pulse oximeter device made a fingerprint the most viable biological key for our system.

Meanwhile, our blockchain team members applied and successfully joined Blockchain at Berkeley, and immersed themselves in the Blockchain at Berkeley scene. They entered into a Blockchain hackathon and won, and met with the mentors in Blockchain at Berkeley to discuss their architecture. From a security standpoint, we had to depart with the current biological models of authentication used for example on the iPhone, because the biological key is stored in the devices as a template that can be used for future comparison. We met with our industry mentor who explained this security model to us and helped coach us through how to understand the security architectures

deployed today. So our team members had to come up with a way that would shield the privacy of the biological key (not store it or expose it), and went through an iteration when their mentors at Blockchain at Berkeley explained that they could not do the bio key processing on the blockchain, as it is by definition public and exposed. They developed a two contract system, which merely stores the public functions on the blockchain, but which does all the key processing in a Javascript front end that is not stored - thereby protecting the individual's confidential data. Finally, the medical record storage on IPFS takes advantage of new technology in peer-to-peer network protocols to encrypt and shard data across a decentralized network, thus enabling fail-over protection and resiliency to all the problems of network centralization.

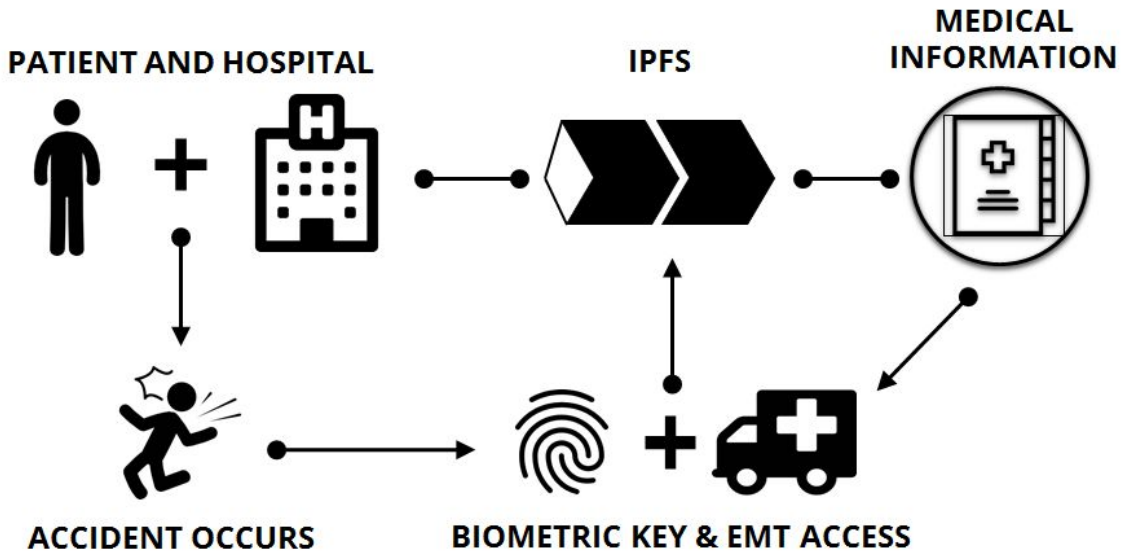

Figure 1. A graphical overview of the proposed project goal

The Solution

We successfully developed a method to use biometric authentication to access medical data through an Ethereum blockchain. The first component of this solution was converting the fingerprint scan to a unique, reproducible key that could be used to identify the patient. We experimented with different methods of performing this task, and ultimately landed on an image pre-processing pipeline and dimensionality reduction of the numerical array representing the image.

We used fingerprints from the VeriFinger database, which was publically accessible. The images were first converted to grayscale. Then we performed histogram equalization to improve the contrast of the images. Essentially, what the equalization step does is "stretch out" an image's histogram so that its pixel intensities are better distributed, allowing areas of lower local contrast to gain a higher contrast. Next, we performed garbor filtering. Garbor filters are linear, orientation-sensitive filters. They are frequently used for edge detection, and we found them to be successful in emphasizing the lines on the fingerprint scans. We utilized an OpenCV implementation of the garbor filter.

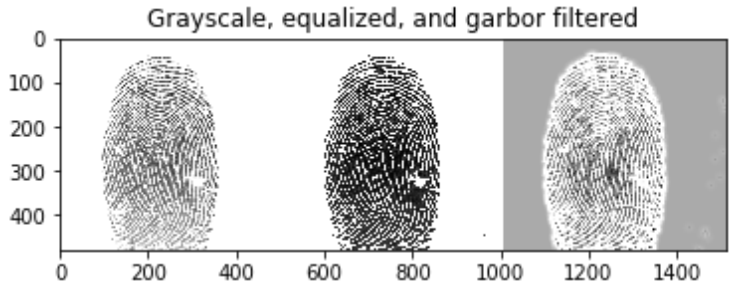

Figure 1. Fingerprint scan pre-processing.

Then, the pre-processed fingerprint image arrays were flattened, which resulted in an array that was over 200,000 integers in length. We performed principal component analysis on the set of flattened image arrays using the scikit-learn implementation of PCA. The first step is to “fit” the PCA, which computes vectors onto which the data is projected, maximizing the variances between each object. The second step is “transform” which transforms each 200k-long image array into their respective scores on the principal component axes. This results in an array of length 9. The floats in this array were converted to integers and the absolute value of these integers was taken. Then, the first digit of each integer was selected and combined into one string of 9 numerical characters. This is the unique key that represents each individual fingerprint. This key is reproducible; when a fingerprint scan is pre-processed and the pre-fit PCA is used to generate the PC scores which are then truncated and fused, this results in the same key. Then, this key is passed into into the blockchain.

On the Ethereum blockchain, we have smart contracts that contain functions that take the key produced by the fingerprint scan and use that key to map the location of the patient’s emergency medical data on the IPFS database. We use both the patient’s index finger and the patient’s thumbprint (the thumbprint key is used to locate the function that maps the patient’s index finger key to the emergency medical records). This system (pictured below) is unlike anything that has been previously developed, and offers a way for medical data to be accessible yet secure. Additionally, we used Javascript React to develop a front-end where patients can upload their medical data and where EMTs can read the retrieved medical records.

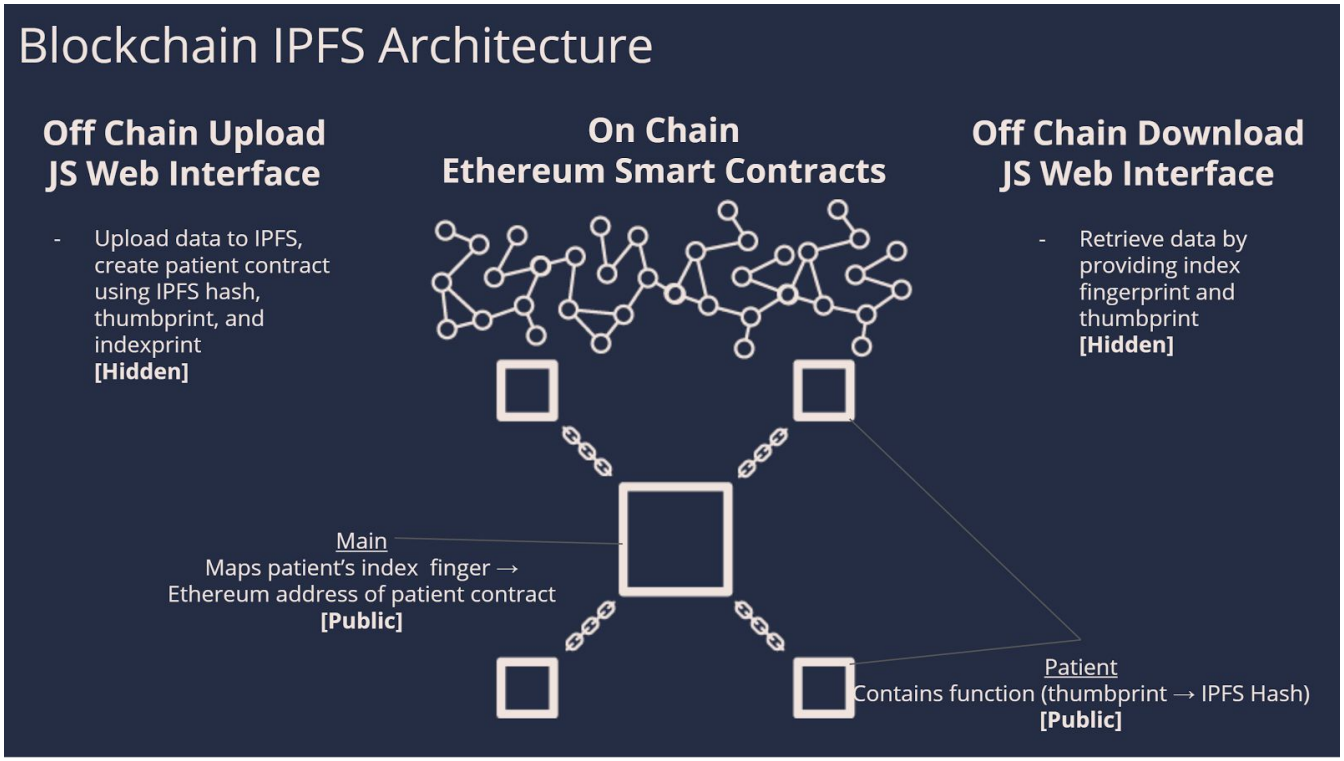

Figure 2. Blockchain & IPFS Architecture

Future Goals:

The potential for future improvements on this project is endless. We aim to develop a piece of fingerprint recognition hardware while partnered with a biomedical emergency device firm - such as Medtronics. Additionally, hospitals and service providers will need to be pitched to and begin to onboard patients onto the technology. Ultimately, the technology will licence software solutions to these hospitals and once the pilot programme reaches a critical mass of patients, we can begin to trial the technology in San Francisco or New Zealand. New Zealand is an especially attractive pilot destination as it is an easy entrypoint into a market that is open to testing. The New Zealand healthcare system is also in many ways more conducive to the technology than in the US.

Team Member Contributions:

Alex Ackroyd
- UI/UX design: flow of architecture and user interface concepts
- Conceptual design

Jessica Yao
- UI/UX design: flow of architecture and user interface concepts
- Conceptual design

Sumayah Rahman
- Fingerprint -> unique hash methodology and code
- Biometric classification code (technique that was not used in the end)

Dat Mai
- Fingerprint -> unique hash methodology and code
- Accuracy improving training for classification technique

Nishaad Navkal

- IPFS architecture design, smart contract creation
- Front end webpage creation

Federico Kunze

- IPFS architecture design, smart contract creation
- Front end webpage creation

Working with Mentors:

Sanjeev Verma - Sanjeev was an invaluable advisor throughout this project. He provided tips and insight into the blockchain portion of the project and truly enhanced the direction of HealthChain. We met Sanjeev through the data-X programme and are extremely thankful for the connection.