Impact Opportunity

According to the latest research from UNHCR, the global refugee population is 22.5 M and an additional 65.6 M people have been forcibly displaced from their homes. While the majority of these refugees come from the Middle East and East Africa, the region our group will focus on is the mounting refugee crisis across Latin America (LATAM). Normally, migrants from LATAM are not considered in traditional refugee relief efforts. Mounting political and economic instability in the region has resulted in a massive growth of LATAM migrants, often under-counted and lacking a formal registry for international aid efforts.

LATAM can leverage the region's shared language for refugee resettlement and aid. "Over the past thirty years, cooperation and regional solidarity in Latin America and the Caribbean have proven effective in dealing with situations of displacement." Brazil Action Plan

There is not a formal registry of LATAM displaced people so specific statistics on demographics are hard to estimate. Globally, the a large portion of refugees are women. Women with small children are especially vulnerable to sexual violence, exploitation and physical insecurity. Remaining challenges identified by UNHCR for LATAM migrants include: access to asylum procedures, access to documentation, and access to services. Education levels vary among the 8.3 M displaced people throughout LATAM.

Political and economic instability in the region has lead to increased refugee populations particularly from Venezuela. UNHCR estimates that 1.5 million Venezuelans are currently displaced in the LATAM region. In Central America, drug wars and gang violence have displaced populations in El Salvador, Honduras and Guatemala, also known as the Northern Triangle. (source). Many other LATAM countries are facing mounting political instability as well. The economic conditions of the LATAM region are most commonly stagnant and in some areas depressed. We must take into consideration a compounding effect in LATAM, that as host countries feel the stress of recent immigrants, they are vulnerable to fall into a similar crisis of instability and hardship.

"Several countries in Central America like Honduras, El Salvador and Guatemala top the list of homicides in the world. The heightening violence there has forced people to flee their homes." [Source](#)

More recently, LATAM is also seeing an influx of migrants from Asia and Africa in attempt to request asylum and refugee status from United States and/or Canada. ([source](#)) Further, it is not out of scope to consider the entirety of Latin America as a possible network as stability often changes in Latin America by the year. For example, in the late 1980s and early 90's, Colombians were crossing the border to Venezuela in droves, fleeing from the violence and poverty in Colombia. However, at present Venezuelans are crossing the border to Colombia in large numbers to escape violence and poverty as well.

Currently, displaced people throughout LATAM have limited resources to address their migration and resettlement efforts. In border towns such as Cúcuta, Colombia, Venezuelan migrants find shelter in soup kitchens, community pantries, churches and makeshift tent-villages. For Central Americans escaping the violence of the Northern Triangle, many resettle in Ecuador or travel north through Mexico seeking asylum in the United States.

Scope Addressed:

In Latin America, refugees and migrants often travel, many times walking, long distances with little or no things. Most of them travel without phones, and it is even less probable that they have access to a smartphone. They are off the grid. Throughout the journey, refugee travelers are exposed to theft, violence, sexual abuse, human trafficking and extortion in Latin America. ([Source](#)) These conditions create a significant challenge in integrating blockchain as a solution. However, our solution takes all of these conditions into consideration. Our solution intends to improve the conditions of refugee and migrant travel from the start of their journey to their end destination by providing refugees with a method to store their savings, information regarding their identity, and communicate with friends and family. Out of scope elements would include the refugee settlement and integration process as well as legal intricacies.

Solution Description

We propose the design of a **Safe Passport**. This "passport" would work similar to a paper wallet with a QR code that will carry several pieces of information, primarily 1) the address of a multisignature wallet, 2) personal information (such as name, age, birth date, citizenship, etc.) and 3) the private key corresponding the migrant's externally owned account. We address the security concerns of carrying this information in a paper QR code through the use of encryption, the use of message authentication codes (MACs), a EURion constellation, halftone QR codes, and required biometric (fingerprint) data for unlocking. The full details of this architecture are laid out later in this paper. By allowing refugees to carry their identity, savings, and personal information along their journey, we intend to reduce migrant and refugee exposure to theft, violence, and extortion in Latin America as they travel throughout the region.

Why is blockchain needed to solve this problem?

As the underlying technology behind cryptocurrencies, blockchain has enabled a whole new system of value transfer that can occur outside the confines of traditional banking. Furthermore, blockchain technology is a powerful record-keeping tool. For many migrants, the traditional options for value storage are subject to uncertainties in fiat currency fluctuations and unstable interest rates. More poignantly, value transfer incurs significant fees in cross border payments. In addition, record-keeping institutions like governments or banks of their origin country are often inefficient, corrupt or inaccessible.

The failures of traditional institutions indicates that a technology like blockchain would be necessary to improve the accessibility to funds and resiliency of record keeping for migrants and refugees. The application of blockchain has been successful in other refugee populations such as Syria ([source](#))

Our tools allow refugees to carry information regarding their identity, store and access their saved funds and share communication with relatives or friends. Through the provision of these services, we are enabling people to enhance their safety while they are traveling in a refugee condition.
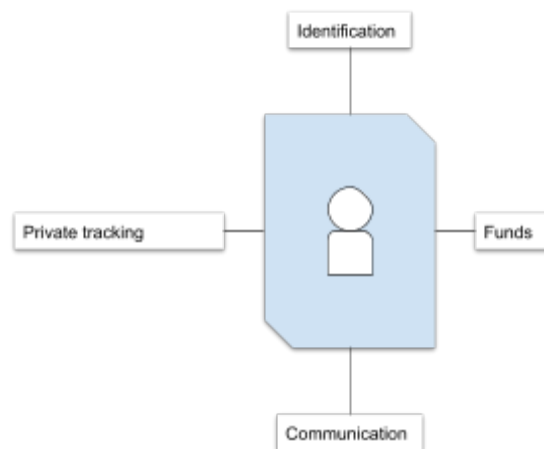
By storing funds using the Ethereum blockchain and with a stable digital currency such as DAI ([source](#)) or TrueUSD ([source](#)), migrants mitigate the risk of losing all savings due to thieves, corrupt authorities or currency fluctuations. After arriving to a migrant shelter, migrants will have access to all of their savings and information via their **Safe Passport**.

Another issue refugees and migrants face during their journeys is the availability of secure communications. Phones are an added expense and the purchase of sim cards specific to each country while crossing borders is impractical. To this end, we propose the use of Ethereum's Whisper protocol. It will let us create a private shelter check-in message which could only be read by the migrant's designated relatives or friends on the platform in order to get more information about the journey. By following the journey, it will become easier to reunite families.

What is the size of the market? What demographics will you serve? Which industries will you impact? Any concurrent trends?

At present, we are considering Latin America, the area where our target market would be, to encompass all countries south of US-Mexico border. A tentative country list can be found [here](#). This area is populated by over 600M people. Though Latin America may only be home to less than 10% of the world, it the location of 33% of the world's homicides ([source](#)). For, example from 2011 to 2014, San Pedro Sula in

Honduras was the deadliest city in the world. In 2016, it was still ranked third.Though Latin America may be rich in natural resources, current poverty and extreme poverty rates are on the order of 30% and 10% respectively and continuing to grow ([source](#)).

According to the UNHCR, there are over 8.3 M people throughout LATAM who are displaced, seeking asylum or otherwise in a refugee-like situation. However, as home to so much violence and so much poverty, as a group, we estimate the number of those who are eligible to meet refugee status in more stable countries in Latin America, such as Mexico, Peru, or Argentina, the US, Canada, and other nations to be much higher than this measure. The two greatest areas of concern are the Northern Triangle of Central America (NTCA) – (El Salvador, Guatemala and Honduras) and Venezuela. (source: [Undocumented Migration in Northern Triangle](#), [UN Refugee Agency 2018 Planning Budget](#), [UNHCR Venezuela Supplemental Report](#)) Focusing on the [Venezuelan situation](#) alone, UNHCR reports that "between 2014 and 2017, over 100,000 asylum claims were lodged, half of which in 2017 alone (as of September)".

As to demographics, we will target the refugee and migrant communities of greatest need as described above in the Northern Triangle of Central America and Venezuela.

The industries potentially impacted would include money transfer organizations, money services, exchanges and to a lesser extent telecommunications. Needless to say, typically the amount of money that migrants in Latin America carry is typically less than $2,000. In light of that information, we do not expect to change or impact a significant portion of any industry, per se, so much as provide a service to refugees and migrants.

Concurrent trends impacting the LATAM region include:

- **Political and Economic Instability**: Examples include the rising inflation rates in Venezuela and the political instability throughout the region.
- **Drug Wars and Gang Violence**: This is evidence by the escalating violence employed drug gangs in Mexico and El Salvador.
- **Increasing Poverty and Increasing Extreme Poverty** ([source](#)).

What are current solutions to the problem you identified? Do they work effective?

Again, to re-emphasize, the problem we have identified is refugee and migrant safety while they travel and are exposed to external risks including theft, violence and extortion.

Currently, displaced people throughout LATAM have limited resources to address their migration and resettlement efforts.

Current "solutions" include:

- Contracting human smugglers
- Staying with extended family

*Note that for the above, we are only addressing the *travel* aspect of refugee and migrant conditions. There are several NGOs and charities that have established efforts in aiding in refugee resettlement; however, solutions for safe travel are not currently available, save through lesser known means.

Currently, these solutions are not effective -- human smugglers are expensive, unreliable and often lead refugees into human trafficking. Although staying with extended family may be a more reliable methodology it is not scalable, and again, nor does it provide any security to the refugee or migrant while traveling.

Who are the stakeholders involved? How are they thinking/feeling/acting currently?

There are various stakeholders we consider in crafting our solution.

- Migrants and Refugees
  - Migrants and refugees looking to travel with a more secure means of handling their savings, identity, and communications can look to our solution to use along their journeys.
  - Currently, these individuals primarily seek help from local friends, family members and perhaps a few lesser known local organizations.
  - They are scared to leave the country they know and grew up in, but escalating violence combined with economic hardship makes it impossible to stay and have a future for themselves or their family. Many will have been victims of political violence or targeted gang violence. Depending on the location and conditions, these individuals' educational background could range from elementary to college level graduates.

- Latin American Local Governments
  - Certain LATAM countries have a history of solidarity with regional migrants. Countries like Ecuador and Colombia issue right to work documentation for recent arrivals. For Venezuelans, Peru and Argentina also readily accept those seeking asylum for certain amounts of time. However, governments are also concerned with the dramatic increase in regional refugees and migrants. Since LATAM is experiencing economic stagnation, insecurity and high unemployment, local communities are expressing concern, anger and fear towards migrants and refugees. These conditions escalating the instability of the region.

- United States Government
  - It would be dismissive to not address the current state of immigration from Latin America to the US via the US-Mexico borders.
  - Frustrations abound on both sides of the equation. The United States government must produce a sustainable and clear immigration policy for refugees from Latin America (and globally) according to the desire of the American voters. Unfortunately, at present, the United States is lacking the bipartisanship support required to come to an amicable solution that is not continuously changed and re-addressed as elected officials move in and out of office.
  - The immigration authorities are currently overloaded and under-resourced in addressing refugee asylum cases.

- Latin American Local Businesses
  - Local business is a key driver for economic stability. In collaboration with local businesses, our solution could enable migrants to participate in local economies through the use of their digital wallet in which their savings are stored. Furthermore, as migrants seek employment, our solution could provide a means of record that allow business owners or hiring managers to ascertain the identity of an individual.
  - Local businesses are hard working and eager to expand. They view refugee immigration as a good thing so long as it does not negatively affect their ongoing operations.

- Refugee Shelters and local charities
  - Due to the transitional nature of the migrant journey in the LATAM region, refugee shelters and local charities stand to gain significant leverage through using a broader regional collaboration to assist the migrants and refugees that they are looking to serve. For example, one shelter can alert another shelter of an impending influx of migrants, and data can be collected on a larger regional basis.

The ambition behind our solution is ultimately global. Once scaled up in Latin America, all displaced populations should benefit from the support our solution provides. In the case of the BSIC hackathon however, we focus on the needs of Latin American migrants, and in particular Northern Triangle of Central America (NTCA) and Venezuelan families relocating to more stable areas.

What are the geopolitical, cultural-social-economic factors that must be taken into consideration? What are some nuances and complexities that must be address?

As stated above in previous questions, there is pervasive economic and political instability throughout Latin America. An additional nuance and complexity in the Latin American region is the escalation of violence. This violence is not the result of warring countries or territories but rather drug and gang violence, which in some areas has become a part of everyday life. In our solution proposal, we are aiming to protect migrants from this economic instability and growing violence.

Business Model Validation

Who are your clients/users? Sketch out the persona of your user.

- Primary Client: Refugees and migrants in LATAM, particularly unaccompanied women and unaccompanied children.

- Secondary Client: Local charities and migrant shelters in host country as well as family and friends of the refugee or migrant.

- Tertiary Client: International donors, NGOs and humanitarian aid organizations.

Example Refugee/Migrant Stories

Name: Maríangela Origin: Venezuela Destination: Chile Age: 24 years Sex: Female Education: High School Marital Status: Married Children: 2 Quote: "I just want to cross [the border] with my kids to a place where I can finally be free, without threats."	Mariangela is traveling from Venezuela with her two children to meet her husband in Chile. She has an android smartphone and $200 in cash. She has a high school education.The bus trip will take her three days of travel. During each of those nights, she will have to find shelter. At these shelters, she will likely not take out her phone for fear of drawing attention as cell phones are an easy target for theft and extortion. Once in Santiago, she will connect with her husband by calling him from an internet cafe via WhatsApp or other phone application. Her main priority is to travel safely with two young children, avoiding theft or violence. She intends to use the $200 cash is for food and shelter along the way, and in a worse case scenario, bribes. The political and economic situation in Venezuela has divided families, including Mariangela's. Her key fears include not knowing anyone that she is traveling with, not knowing who to trust, not being able to use her phone during travel, not having safe shelter overnight.
Name: Jennifer Origin: Honduras Destination: US Age: 14 Gender: Female Marital Status: unmarried Children: 0 Quote: "I'm feeling happy, but nervous at the same time. What if they don't give	Jennifer is from la Ceiba Hondura, a city rife with drug trafficking where some children have to travel to USA and bring back drugs to be able to cross to the USA alive. Drugs have become the only insurance. Jennifer is traveling north through Mexico to eventually reach the US. She has family in Texas but does not know how to reach them. She is traveling with a group of other young children (boys and girls) aged 10 to 20 years old. No one in her group has a cellphone or any cash. They were robbed on the border of Mexico and Guatemala, the most dangerous border.

us asylum and send us back to our country?"	At one point in the journey, Jennifer and her group might come in contact with a human smuggler. Her main priority is to escape gang violence and start working. Her pain points are having no cash, no knowledge of where to travel, little formal education, and no way of establishing contact with relatives. Jennifer and her group have to make most of the journey on foot.
Name: Beatriz Age: 47 Gender: Female Marital Status: married Children: 4	Beatriz runs a soup kitchen in Roraima, a border region between Venezuela and Brazil. (source) She is an active church goer and helps migrants who are traveling on foot from Venezuela. She has a college education, a home with wifi. Her four adult children live in Colombia. She uses the internet to help run a small business. Her pain points are that there is no central NGO or authority to help with the migrant crisis in her region. She serves many people each week through informal community networks. She knows that the government of Brazil has committed to distributing aid and funds to the community of Roraima but information about migrant programs not well-distributed. She does not have a record of who comes through her soup kitchen or her church so defining the extent of the challenge proves ambiguous. She also knows that many migrants crossing the border will have a language barrier if they resettle in other parts of Brazil.

Quotes are from real immigrant stories. (source)

Here we provide a collection of stories following the journey of migrants. This will help identify, map, and illustrate pain points.

- Centroamerica to USA (English, video)
- Nour, from Turkey to Gothenburg
- From Piraeus to Munich
- 2017 UNHCR Report: Migrant Risks in Europe
- 2016 UNICEF Report Child Migrant Risks
- OpenMigration Reports on Human Trafficking
- Articulo sobre Migrantes Centroamericanas (Spanish, article)
- 2018 Amnesty International, Refoulement Mexico
- FMReview, Challenges with Migrants and Mobile Phones
- UNHCR Open Portal Refugee Data
- Mesoamerican Social Networks for Migrant Women
- Special Report on Children Migrants (Spanish, article)

Shelter Databases: here and here

What are their pain points? How does your solution solve them?

Primary User Pain Points (Refugee/Migrant):

The journey of leaving one's country of origin is fraught with challenges. Often, the final destination is known and the journey is made by foot or with human smugglers ([source](#)). Migrants are vulnerable to extortion, corruption, and armed robbery. Often traveling with young children or cash, migrants are targets for gangs and at risk of human trafficking, kidnapping and sexual violence. Throughout the long journey, migrants frequently lose contact with relatives and travel companions.

Pain Point	Solution + Unique Value Proposition
Valuables attract attention and the increase likelihood of theft or violence.	Our solution uses a discrete QR code in which a digital wallet is hidden in a photograph using steganography techniques. This way users can store savings in the wallet at the beginning of their journey and exchange it later once they arrive to a safe shelter.
Maintaining contact with relatives and friends while traveling	Our solution allows users to send and receive messages when they check into respective locations that use the platform. It also enables relatives to follow the migrant's journey as they check in to various shelters or partner locations.
Identification and documentation	The QR code will also include encrypted personal information. It will be a temporary ID which can be upgraded to a more permanent identification.
Storage of Funds	The digital wallet for which we will produce a paper wallet, allows migrants to securely store savings.

Secondary Client Pain Points (Local charities, migrant shelters, family and friends):

Pain Point	Solution + Unique Value Proposition
Contact with refugees and migrants during travel	Our solution intends to combine a network of local organizations to use the platform. We do have elements within our system that allow messages to be sent and received when connected.
Weak collaboration between organizations	There are independent organizations that could benefit through aligning themselves with other organizations in different cities or even different countries. Our system brings together multiple organizations to create a network to support refugees and migrants.
Record keeping and data collection	Robust systems are expensive and time consuming to design and implement. Most charities and NGOs do not have a strong system for recording and collecting data. Our system would provide a way for these organizations to safely collect and organize data via the Ethereum blockchain.

Tertiary Client Pain Points (International donors, NGOs and humanitarian aid organizations):

Pain Point	Solution + Unique Value Proposition
Lack of knowledge of where to direct funds	Donors and larger humanitarian organizations are often challenged when attempting to find an effective and trustworthy organization to fund. Our system would set up a network of verified local organizations that would be strong candidates for more funding.
Weak record and data collection.	The United Nations and other larger humanitarian organizations are consistently struggling to find up to date and verifiable data. Our system would help to contribute to this necessary record keeping that could ultimately help organizations where more aid is needed and where it is most effective.

Does your solution depend on context? Can it be scaled?

As stated above, our solution leverages the LATAM context of shared language and historically migrant-friendly host countries. However, it can be scaled to other support regions. Ultimately, once a strong platform and system is built out, it can be used in other regions with a similar network of local organizations that are supporting migrants and refugees.

What is your go-to-market strategy? Who can you partner with?

To begin, we intend to establish partnerships with local shelters in México, Venezuela and USA. While gathering these partnerships a technical team will be creating an MVP to test with early partners. Also, we intend to conduct interviews with experts to talk about migrant's paints points and about our solutions. Once initial partnerships have establish and we have tested the MVP, these entities will collect feedback from people using our service so that we can re-iterate and improve the product.

The next phase of our strategy focus on positioning our solution within local communities of migrants as a tool made specifically for them and by an organization they can trust. We also want to establish our organization position in the international aid community to garner support and buy-in from larger shelter networks.

Finally, our strategy would involve organic growth and word of mouth referrals as more people use our solution and see its value. Marketing products to vulnerable populations is not our objective. We want to see the solution grow if and only if it provides tangible value to our end users.

Potential Partnerships:

There will eventually arise a need to exchange cryptocurrencies for fiat outside of our network of established organizations. To accomplish this task we would need to partner with exchanges, banks and merchants.

- Banco Azteca - Bank with coverage all over Central and part of North America. It can help us to get refugees onboard and act as a support center. Banco Azteca's clients are people at the base of the pyramid.
- AirTM is a solution that can help us to get refugees onboard. It will enable them to buy and exchange a stable cryptocurrency which will be loaded into our wallet.
- Bitso - Mexican cryptocurrency exchange. It will become a great partner on enabling cash out. It will be very useful for shelters and establishments.
- Small supermarket chains can also be very helpful because of their locations and national coverage.

How will your product generate revenue? Will it be financially sustainable in the long term?

As our solution is first and foremost a charitable humanitarian effort, our product is not revenue generating, and we do not plan on charging any fees to use the platform. However, the team will obviously need a way to fund not only the technical build of this proposed solution but also the business side of setting up partnerships with local organizations, verifying legal requirements, etc.

Traditional methods of fundraising are available through grants from governments or fundations, sponsorships from private or multilateral organizations and partnerships with actors established in the ecosystem.

However, we propose a token sale to fund our platform build out. Before uncertainties arise, let us go through the rationale as to why this would beneficial for our project.

First, our smart contract system, which includes the digital wallet and smart contract registration system, will be on Ethereum. At this point, although we do intend to reduce gas usage to a minimal amount through the use of signed transactions and gas efficient contract design, any local organization or refugee/migrant interested in using the platform will need to own even just a minimal amount of Ether for gas to utilize the platform. In raising Ether through a token sale, the core project team is able to send Ether directly to local organizations using the platform so that 1) they do not have to pay for platform usage and 2) do not have to find a way to exchange fiat currency for Ether.

More importantly, we envision that refugees and migrants will use the digital wallet portion of our solution to store their savings - ultimately in a stable currency, not Ether. This presents a challenge for the refugee or migrant to exchange fiat currency for cryptocurrency -- a highly impractical ask. However, by raising Ether, we intend to locally exchange fiat for crypto at the local organizations that the refugees or migrants would approach for the creation of the wallet and *Safe Passport*. This means a migrant could go to their respective organization to set up their wallet with their funds and exchange them for crypto onsite while avoiding expensive fees from most traditional exchanges. Although legal ramifications would need to be addressed, as stated before, most migrants travel with $2,000 or less -- at low exchange amount, we do not write off the possibility of making this happen.

Lastly, what would be the use of the token? The contributions would be charity to build the platform and fund the organization, and the token certainly would not be traded on any secondary market. Furthermore, we would not be using the token as a utility to power the platform as there is no need to do that and incentivise any sort of crypto-economic system. However, we would like to set up a governance mechanism for the token in which holders can vote on the direction of the organization and the usage of funds. In this way, we can engage donors and build a decentralized form of governance into our platform. In light of this goal, our KYC process for contributors would need to ensure a vested interest in the success of the platform as a nonprofit solution and not a revenue generating organization.

In the first year, the LATAM group will hold onto a large enough amount of tokens, so that the foundational elements of the platform are built as promised in the token sale advertising. Following the foundational build out, more tokens can be sold from the LATAM team, and that would allow for larger participation from the donor side.

What are the implicit and explicit assumptions being made in your business and financial model (user-profiles, partnerships, costs, etc.)? How do you plan on validating them.

Our initial assumption is that we will have partnership with migrant shelters to test our MVP. We also assume that we will be able to build a strong network of shelters, charities, and NGOs that would want to be a part of and participate in our platform.

We assume several characteristics of the target migrant population we wish to serve:
- that they have cash (that they will need to store at least a portion of while they migrate)
- that they have relatives or contacts (whom they will be in communication with)
- that they meet legal requirements migrating to their final destination or requesting asylum as we would not want to support illegal activity

We assume that although the regulatory environment for the possession and trading of cryptocurrencies continues to evolve in Latin America, ultimately, this region will adopt policies similar to that of the United States and Europe in which possession and trading of cryptocurrency is not illegal, but regulated.
In fact, Mexico has been a pioneer in this revolution. A couple months ago, the fintech law opened an amazing opportunity for the crypto ecosystem, in which *"Banking institutions may carry out transactions with the virtual assets determined by the Mexican Central Bank through enabling regulation, with the prior authorization of the Mexican Central Bank."* ([source](#))

In terms of cost, the initial build out of this project would be a multi-million dollar initiative requiring several resources from the technical side, the business side, and the legal side. Costs estimates would need to be outlined in detail (+/- 5%) in order to hold an accountable token sale for donors. Furthermore, we would need to established a methodology for recurring donations or receipt of grants or other funds. We would need to estimate the recurring annual costs to maintain the platform and the organization once established. Also, once validated, we would determine a detailed plan on how to raise money and implement our solution in other regions.

What is the vision for your product? Can it significantly change the current state?

Our vision is that this **Safe Passport** solution will aid refugees and migrants in their journey by connecting them to a network of trusted resource providers (such as refugee centers, hospitals, etc), enable them to maintain an identity while securely storing savings and funds, and facilitate secure communication with NGOs, friends and family.

Currently, during their journeys, refugees are unprotected from malicious actors and disconnected from family, friends, and organizations that could provide aid - whether that be law enforcement, hospitals, or a network of NGOs, etc. Though there are established and legal refugee programs, these programs are currently broken from dishonesty, uncertainty, and opportunistic offenders on both sides of the equation. Our platform intends to start to form a trusted network to support refugees and enable refugee programs to reduce inefficiencies and corruption.

Our fundamental belief is that freedom from discrimination and the assurance of equality of opportunity form the basic rights to build a peaceful and democratic society. With that freedom from violence and persecution must also be present.

We don't choose where and what conditions we are born into.
We want to empower people to achieve their potential and a good quality of life.
Everyone deserves the right to a happy, meaningful and safe life.
Everyone's voice should be heard.
Refugees should benefit from the same opportunities.

Enabling access to the digital and trustworthy world is one of our greatest ambitions. This goal can be accomplished with the Ethereum blockchain.

By providing this solution, we see the potential to significantly change the situation for the disadvantaged refugees and migrants in Latin America, a drastically underserved region. We envision reducing corrupt human smuggler trafficking through providing migrants with an alternative by establishing a trusted network of resources and organizations. We also envision reducing the occurrence of theft and total loss of funds along a migrant's journey.

Technical Architecture

The main component of our system is as described above:

*We propose the design of a **Safe Passport**. This "passport" would work similar to a paper wallet with a QR code that will carry several pieces of information, primarily 1) the address of a multisignature wallet, 2) personal information (such as name, age, citizenship, etc.) and 3) the private key corresponding the migrant's externally owned account. We address the security concerns of carrying this information in a paper QR code through the use of encryption, the use of message authentication codes (MACs), a EURion constellation, halftone QR codes, and required biometric data for unlocking. The full details of this architecture are laid out later in this paper. By allowing refugees to carry their identity, savings, and personal information along their journey, we intend to reduce migrant and refugee exposure to theft, violence, and extortion in Latin America as they travel throughout the region.*
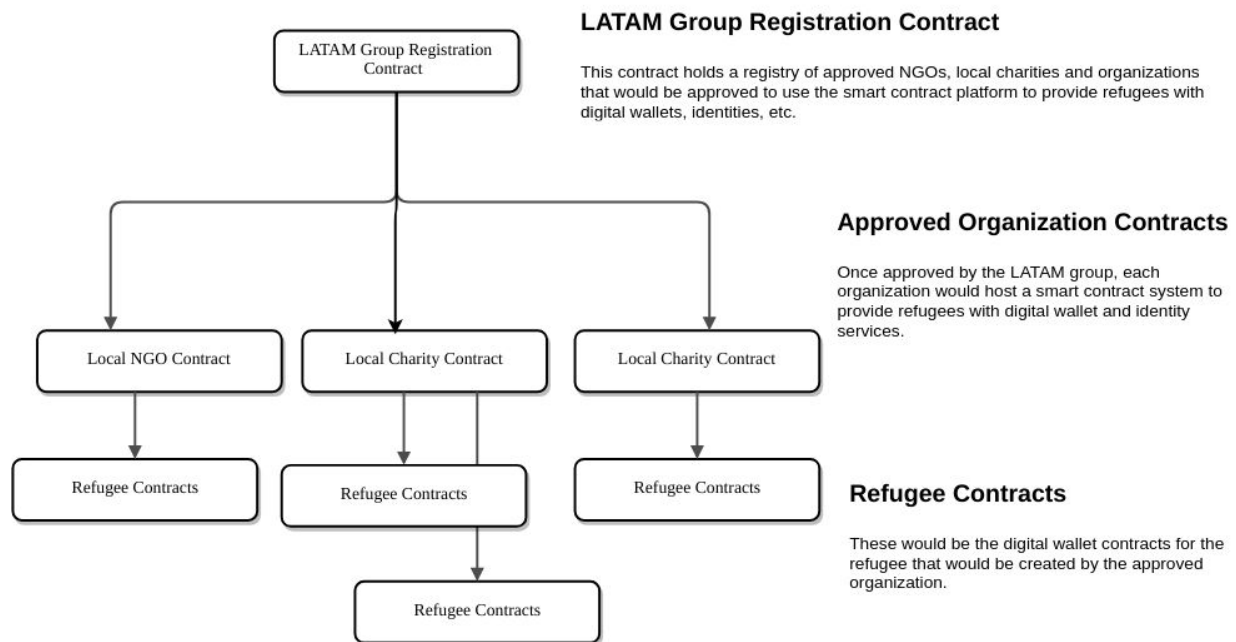
In order to deliver on the **Safe Passport** as described, we envision the creation of a common system for NGOs and migrants, enabling everyone to benefit through collaboration.

In our design, we will put together a system in which shelters, NGOs, or other charity organizations that are validated as trusted will be able to participate in the platform. Considering the amplified risk of the inclusion of bad actors, it is necessary that criteria is established such that only trusted and accountable organizations will be able to participate. For example, in the Latin American region, there is a high number of human trafficking organizations and those whose funding either goes towards or comes from the illegal drug trade. These illicit organizations are often highly organized and may even have a "trusted" presence in the community. However, these criminal organizations are extremely harmful to those in a refugee or migrant status - often enslaving individuals in poor working conditions, subjecting individuals to sexual abuse, and extorting individuals and families out of their life's savings. In order to filter out these bad actors, certain off-chain criteria must be met such as verified financial disclosures, background checks, etc. In this way, we can approve individual organizations and set up a trusted and validated network of actors on our platform.
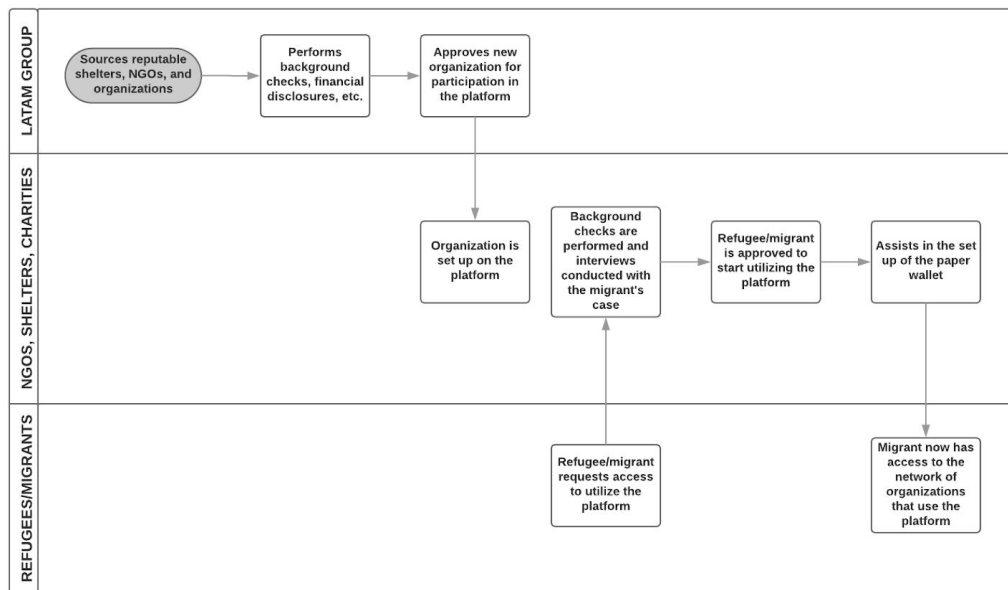
Once validated and approved, the organizations participating in the platform would in turn be aiding in the verification of those migrants or refugees wanting to utilize the platform. A question might arise as to why migrants or refugees would need to be validated, and the answer can be summarized in a few components. First, it is important that our solution is not seen as a facilitation to illegal immigration with a flippant regard for borders or legal immigration efforts. We cannot let any person who might desire to relocate just for the sake of relocation utilize the platform, there must be a valid refugee case or immigration protocol followed. Secondly, in the Latin American region, we need to be cautious when allowing for the transmission of funds that any illegal trade is not able to participate in or access the platform.

Our smart contract platform will use the OpenZeppelin smart contracts and the Gnosis Multi-Signature wallet, both of which have been audited and tested. Furthermore, we will build out a system of smart contracts to manage the registration of shelters/organizations as well as individuals to the platform.

The smart contract registration design will mirror the design below:

LATAM Group Registration Contract

This contract holds a registry of approved NGOs, local charities and organizations that would be approved to use the smart contract platform to provide refugees with digital wallets, identities, etc.

```
              ┌──────────────────────────┐
              │ LATAM Group Registration │
              │        Contract          │
              └────────────┬─────────────┘
        ┌──────────────────┼──────────────────┐
        ▼                  ▼                  ▼
┌────────────────┐ ┌────────────────┐ ┌────────────────┐
│ Local NGO      │ │ Local Charity  │ │ Local Charity  │
│ Contract       │ │ Contract       │ │ Contract       │
└───────┬────────┘ └───┬────────┬───┘ └───────┬────────┘
        ▼              ▼        │             ▼
┌────────────────┐ ┌──────────────┐  ┌────────────────┐
│ Refugee        │ │ Refugee      │  │ Refugee        │
│ Contracts      │ │ Contracts    │  │ Contracts      │
└────────────────┘ └──────────────┘  └────────────────┘
                          ▼
                  ┌──────────────┐
                  │ Refugee      │
                  │ Contracts    │
                  └──────────────┘
```

Approved Organization Contracts

Once approved by the LATAM group, each organization would host a smart contract system to provide refugees with digital wallet and identity services.

Refugee Contracts

These would be the digital wallet contracts for the refugee that would be created by the approved organization.

Generalized Flow of Access, Approval and Participation in the Platform

Registration Portal:

The registration portal will be used to add more organizations to the platform. It will be implemented through the usage of a smart contracts as described above and a secure portal only available to affiliated organizations. It will also be the portal to start the refugees onboarding process. The organizations will be responsible for verifying the input data required from the refugee or migrant.
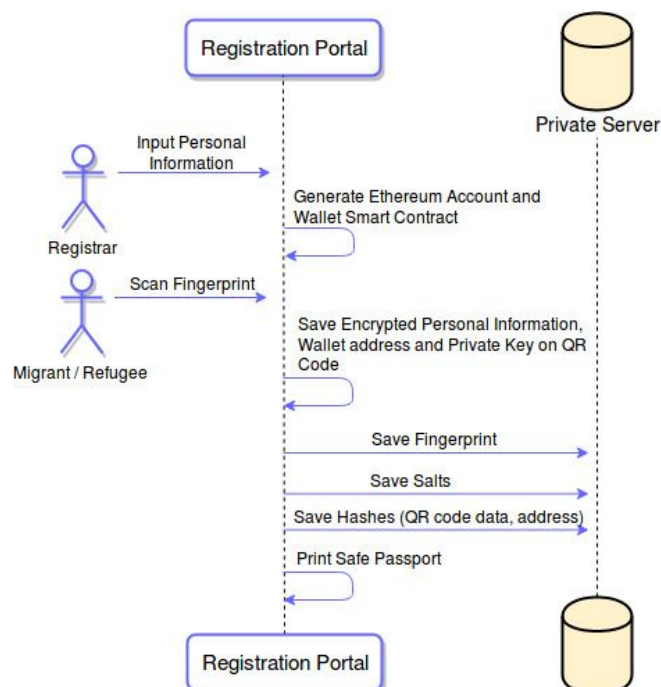
Ethereum Access:

A key element for our platform's success, requires to enable refugees, NGOs and shelters to interact with the blockchain in an easy way. The access portal is a redesigned fork from MyEtherWallet with more beneficial capabilities for migrants/refugees and NGOs.

It can be accessed online, connected to INFURA's servers or a similar provider. A local installation is possible with all of its dependencies and connected to ethereum using the geth client.

The portal will also communication system components to be detailed in a later section. INFURA and similar services have limitations for the Ethereum Whisper protocol. In case of using the communication system, it could be better to use a local installation.

Using private keys on a public computer increments the risk of letting an attacker to log the keys or read the computer memory.

As a security feature, we plan to study and find a way to include Intel SGX Enclave technology or its equivalents to add a security layer for managing private information. No unauthorized access or memory snooping of the enclave is possible.

 Intel SGX Enclave
   1. App runs and creates the enclave, which is placed in trusted memory
   2. Trusted function is called, execution transitioned to the enclave
   3. Enclave sees all process data in clear; external access to enclave data is denied
   4. Trusted function returns enclave data
   5. Application continues normal execution

Externally Owned Public Address & Private Keys:

When a refugee or migrant arrives at an organization to get set up on the platform with a **Safe Passport**, the organization will first help them generate an externally owned public address on the Ethereum blockchain. With that, the refugee will now have a public address and private key to execute transactions on the Ethereum blockchain.

Multi-Signature Wallet Properties:

After the generation of a public address, the organization will help a refugee or migrant get set up with a multisignature wallet. We propose the use of a multisignature wallet so that one wallet may be shared among family, relatives or any other party that the refugee would legally consent to storing funds with (i.e. very close friends that they may be traveling with).

In order to follow American and Latin American standards for Anti Money Laundry (AML). The wallet will use the minimums limit required by both legal frameworks. Also in the very first stage we want to test the wallet with smaller amounts because we want to deter bad actors from using this tool as a method for

drug money trafficking or money laundering. The values below are tentative and dependant on a more indepth legal review in which the best case scenario is considered for the refugee or migrant side as well as legal restrictions.

Wallet Limitations:
- Limit the balance in the account to $2,500 USD.
- Limit deposit monthly to 2,500. USD , which means the limit of cash out and cash in it is the same amount so that larger amounts cannot be funneled through the wallet through multiple withdrawal and deposits.
- Monthly withdrawals limit to 2,500.USD.
- Following the Latin American standards for relevant banking operations, the amount that can be transferred to the wallet **each day** from outside actors as a preventive measure against money laundering is $500 USD, around 10,000.00 mexican pesos. However, migrants may still deposit their own cash in higher values via the organizations that are participants in the platform in the higher range of the $2,500 per month deposit limit.
- Limit the daily amount of withdrawals or transactional in order to enhance the refugee safety ($400 USD).
- Multisignature or validation protocol to add a security layer.

We intend to use the Gnosis Multi Signature wallet as this wallet is audited and has most of the requirements needed for our use case. Additional extensions would be required to support additional and would be security audited as well.

On-Chain Identity Properties:

The on-chain identity will be based on uPort's core components. It is implemented as an Ethereum account to represent the refugee's identity. For On-Chain extended features, the ID will interact with the Ethereum DID Registry.

This feature is based on the "Lightweight Identity" (ERC 1056).

Lightweight Identity Features:
- Delegate: An address (identity) that is delegated for a specific time to perform some sort of function on behalf of an identity.
- Change Owner: Sets the owner of the given identity to another ethereum account.
- Attributes: Contain simple data about the identity. They can be managed only by the owner of the identity.
- Upgrades: Includes a mechanism to update the identity in a cost effective manner

Claims will be created on the claim registry (ERC 780) to record a signed statement, i.e. Maríangela teached english at <X> migrant shelter.

SInce storing identity information on-chain is both costly and impractical given the public nature of Ethereum. We will store a few pieces of personal identification information solely within the QR code itself. This information will be encrypted for privacy. Information to include would be name, age, citizenship, gender, etc. Unique information from each country location may be helpful as well - such as ID card number, passport number, or driver's license number; however, we will need to verify with a legal team the ramifications and risk of storing that type of data.

Accessing Information Contained in the QR Code:

We propose using biometrics to link and unlock QR code data. The biometric data will remain secure on a server and will be audited by security experts.

At each time of access a refugee or migrant, will likely not want to open every type of information within the QR code.

We propose that two set of information be encrypted separately:

Data Set 1:
1. The private keys of the migrant's externally owned account, from which the public address can be derived.
2. The multi-signature wallet address.

Data Set 2:
1. The personal information stored in the QR code.

Each data set will be encrypted within the QR code. Data Set 1 will be unlocked when a user wants to access funds or verify on-chain identity. Data Set 2 will be accessed when a user wants to verify off chain identity. We can use different sets of biometric data to unlock each data set. For example, the right handed index finger may unlock Data Set 1 while the left handed index finger may unlock Data Set 2.

We acknowledge that the information must be under personal control. The biometric data will be anonymized. Personal information (name, date of birth, citizenship, place of birth, gender) will remain solely within the QR code encrypted.

Per each identity there is only anonymized data stored on the server:
1. The biometric fingerprints data
2. Salt 1 of Data Set 1
3. Salt 2 of Data Set 2
4. Hash of the final QR Code Data (MAC-SHA3)).
5. Hash of the Ethereum public address.

Typically, a secure approach to storing a "password" or sensitive piece of information on a server is to hash the password plus a random sequence of characters/numbers called a "salt". The salt is usually

stored on a database in conjunction with the hashed password. To grant access, the user needs to enter the password and the system will hash it along with the salt as a method to verify the correct credentials. The final result will be an identical hash to the one created at the beginning for storage.

We will use a similar approach for encrypting our QR code data. We will use the BCrypt hash of the password plus the salt to create an AES encryption key used to encrypt the QR code data. The rest of the output, the algorithm indicators and the salt, are stored on the server.

[Algorithm] + [Algorithm Option] + [Salt] + [Hashed Password] = BCrypt("Plain Text Password")

$2y$10$6z7GKa9kpDN7KC3ICW1Hi.fdO/to7Y/x36WUKNPOIndHdkdR9Ae3K

└── Salt

└── Hashed password

└── Algorithm options (eg cost)

└── Algorithm

From the string above, we only need to use the [Hashed Password] section to encrypt the data using the AES algorithm. The [Algorithm] and [Algorithm Options] are BCrypt parameters. The [Algorithm], [Algorithm Options], and the [Salt] will be stored on the server as they are required to recreate the [Hashed Password] section.

An optional 2FA could be enabled. However, we again need to consider that many migrants and refugees travel throughout Latin America without a phone, much less a smartphone or a computer. For that reason, a 2FA will not be a primary method through which we achieve security. 2FA could be enabled at the time of generating the paper wallet. It would require the mobile phone number or email of the migrant or refugee in order to receive a message.

QR Code Encryption Data Unlocking Process:

The below diagram shows the process flow of unlocking QR code data.
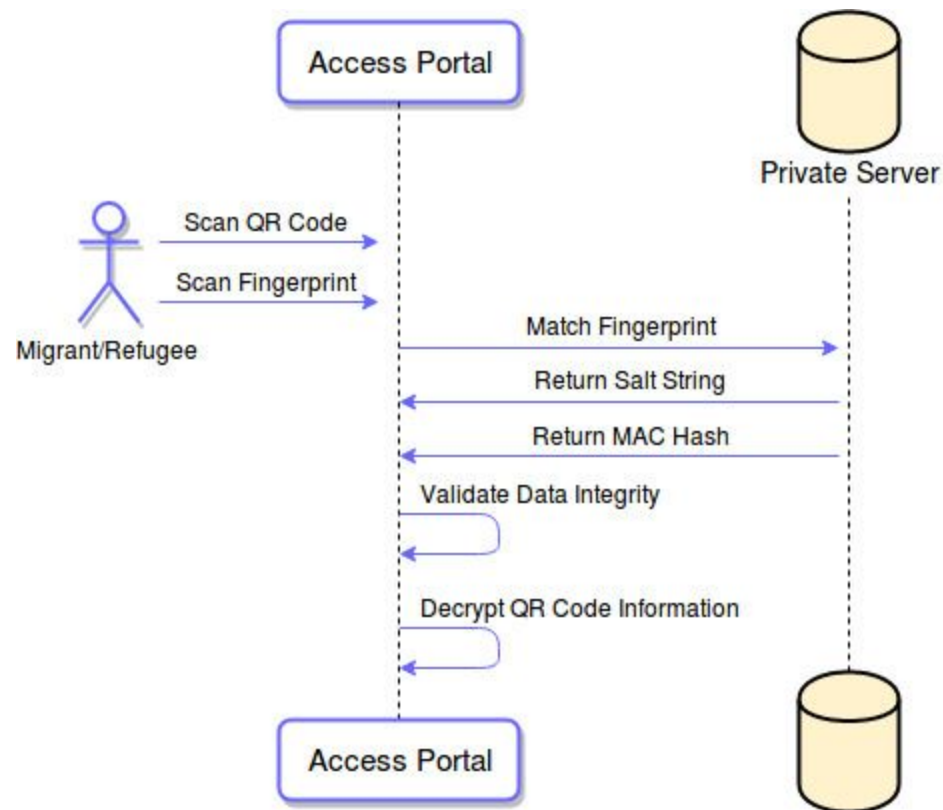
QR Code Anatomy:

The QR code data also utilizes a message authentication code (MAC) that would be generated upon creation in order to validate the data integrity and protect against message forgery. This method we will provide assurance that the data has not been changed and the hash has not been replaced on an MITM attack.

The MAC hash will be stored on the server and compared to the hashed data from the QR code before triggering any action.
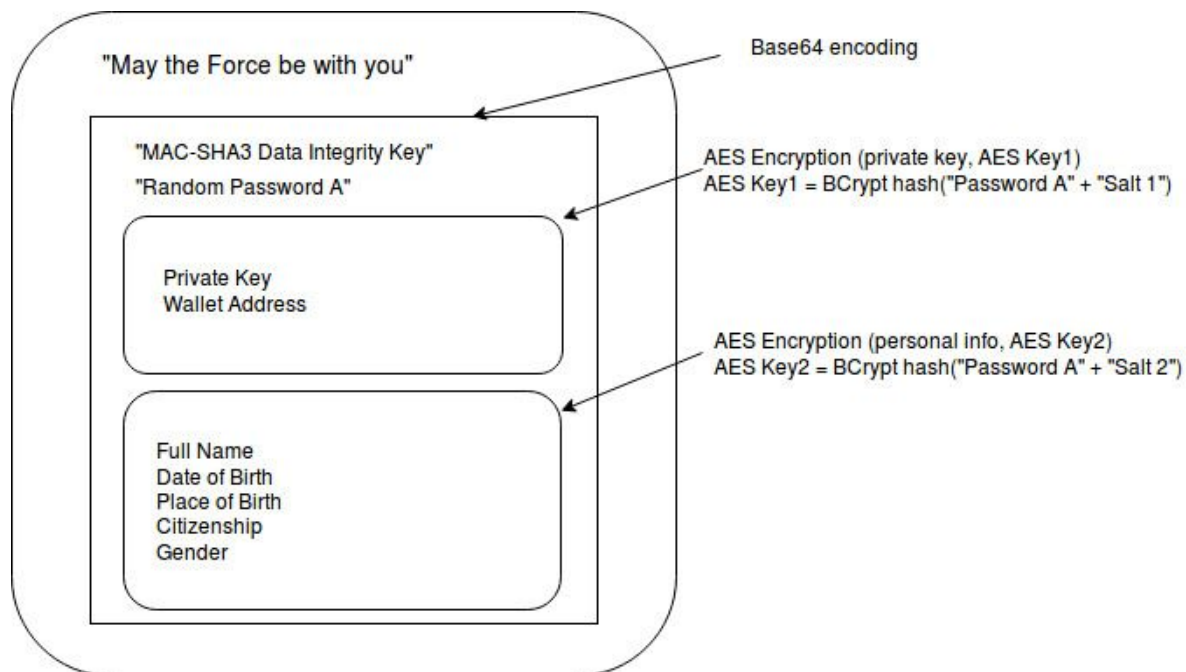
Eg.
Scanned QR Code Data:

May the Force be with you
P6LYzR3X9cAEg++MDtRrOV6kZTZBstggrH2PwT0bQ3g=

In this example, the data is encrypted with an AES 256 algorithm without a salt.
Password (AES key): LATAM -> (the final key will be the hashed password)
The first phrase from the QR code data will be ignored in order to decrypt the message, but it helps to make the code less suspicious if someone scans it.

Refugees will be able to decide what information to use or share. By using different fingerprints they will have the precise control on what information will be decrypted (Private Key, Personal Information) as explained above.

Smart Passport Examples:

As a preventive measure against photocopying, the postcard will have an [EURion Constellation](#).The EURion Constellation is a specific design, typically used on currency that, if detected, in professional editing software, such as Adobe, does not allow the user to photocopy or make any edits.

Religious Iconography --
The Virgin Mary is a prominent figure in the Catholic Church in Latin America. It is not uncommon for one to carry images of the Virgin Mary in a wallet or pocket. Hence, we believe carrying a QR code on this image such as this would be less inconspicuous for traveling refugees or migrants than carrying solely a random QR code.

Halftone QR Codes --
Halftone QR codes allow you to overlay an image with a QR code. The QR code is still left machine readable, yet the overall picture would blend in more to a collection as exemplified by the religious example above and leave migrants and refugees with additional options for carrying the QR codes.
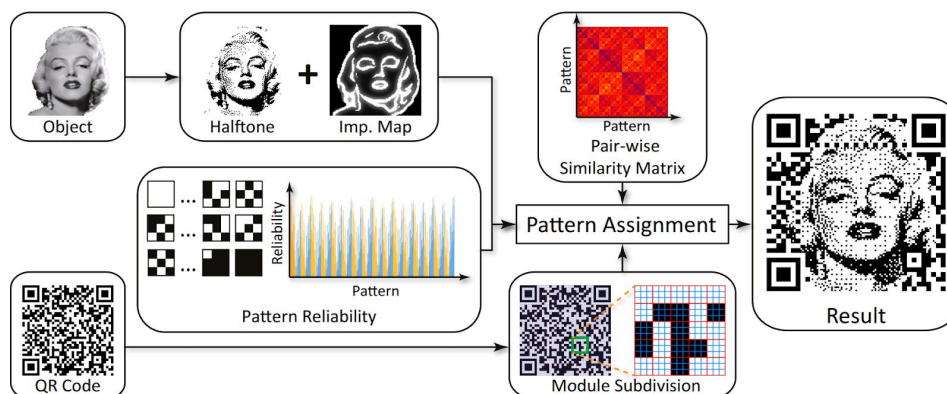

([Source](#))

Communication System

Tor is a great tool to enhance privacy and communication which allow people to communicate in oppressive regimes. But it is a complicated and unstable protocol with which to build a dApp in conjunction. A similar level of privacy and censorship resistant could be achieved by using the Ethereum Whisper protocol. It will let us create a private shelter check-in which could only be read by the refugee relatives or friends in order to get more information about the refugee actual situation.It will create an automatic private check-in message (shelter name, location, time, data) which will be sent as a encrypted message to relatives or friends.

Another feature will enable refugees to communicate with NGOs and shelters in a private channel. Opening this private communication channels, could bring several benefits. Refugees could ask for information, support or help if they feel at risk. Shelters and NGOs will benefit if they have more open channels and can plan better at the moment they are contacted by refugees before they get there.
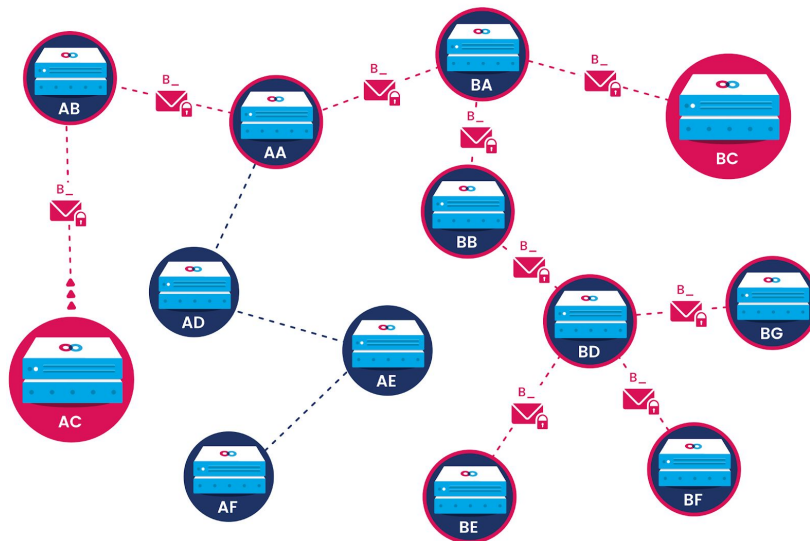
- Every message is delivered to every node.
- Each node sends the message to neighboring nodes, but only the recipient who has the key can decrypt it. All nodes continue forwarding the message to nearby nodes. Even the recipient forwards it after receiving it (untraceability) .
- It's an identity-based messaging system, designed for easy and efficient broadcasting, and also for low-level asynchronous communications (publish/subscribe)

We also plan to use the Whisper Mail Server to keep messages visible and accessible for a necessary amount of time. As a future improvement, we plan to include video or audio calls. This could be done by integrating a voip client or and existing service like Skype.

Wallet Recovery

In case of the refugee death or loss of their **Safe Passport**, we propose a recovery mechanism based on Shamir's Secret Sharing.

We are going to split the private key into several parts. The key could be split into 4 parts. It is possible to recreate the original private key by using 3 of those parts. These parts could be spread among several NGOs, relatives, refugees (Studying the best case will be part of the development).

On a Linux platform, it could be done by following the next steps.

- Split:

```
>$ ssss-split -t 3 -n 4 "KEY"
```

The number after -t refer to how many shares are required in order to re-assemble the key, and the number after -n represents how many shares to generate in total.

- Combine (the order doesn't matter):

```
>$ ssss-combine -t 3 "p4" "p2" "p3"
```

An alternative to this methodology could be through the use of the multisignature wallet to extend access to a trusted third party to access the funds in a worst case scenario.

Right to be forgotten

Legal compliance is a requirement of the platform. We want to give the refugees the right to control their identity. Since there is a central point in our design, we will enable a mechanism to delete their data from the server. To delete the data, the refugees will send a delete petition and authenticate with their biometric fingerprint data on the server. The server will send a random secret message which will be signed by the refugees using their private key. From the signed message, the public address will be extracted and compared with the biometric linked data. After matching the address, the data will be deleted.

Impact Measurement

What is the impact goal of your solution? How do you ensure to capture needs of those who are traditionally underserved within your category?

Our solution is focused for the Latin America region - a region with significant displacement movement as a result of economic and violent pressures are particular regions (i.e. Venezuela, El Salvador, Guatemala, etc). However, in light of regions that are experiencing hardship in a global platform, Latin America is often overlooked and underestimated. For example, nearly 4M people have left Venezuela in light of the economic crisis - a number that closely follows the 5.5M that have left Syria. (https://www.cnbc.com/2018/02/19/venezuela-refugee-crisis-could-be-worse-than-syria-economist.html).

One of the main challenges facing migrants in Latin America is that journeys are often made by foot, car, or bus over long distances and several borders. The length and location of these travels place the migrant in a precarious position when it comes to securing funds along the journey. Although a migrant may attempt to prepare financially, cash is often stolen and lost to local gangs, mafias or other criminal organizations.

Our solution focuses on providing a way for migrants to store their funds during the travels from one location to another. By building a network of organizations that will help migrants set up their wallets and establishments that will accept these funds, migrants can experience a safer, more well connected journey, especially in light of the fact that many migrants in Latin America do not travel with a smart phones In addition, our **Safe Passport** solution will also include pieces of information that could contribute to building a refugee or migrant's identity. We recognize that ultimately, to be of use, identities must be accepted by government organizations, so we intend to eventually work with governments to ensure our identities could be accepted in some manner for legal verification.

Also, we recognize that there is a number of migrants who may become lost or even perish along the journey to their final destination (source). We intend to use the communication aspect of our platform to reduce this number by providing communications through which migrants in trouble may reach out for assistance to a trusted network of organizations.

Within the team we have three Spanish speakers that can help us connect with organizations in Latin America as well as interview migrant or refugees who would ultimately use the platform as well. Throughout the region, we are trying to serve a population that is largely overlooked in terms of refugee and resettlement efforts. We aim to shine a light on the Latin American region and provide a way for refugees and migrants to get help.