Blockchain-based Global Refugee Monitoring Platform

December 2018

Overview

The global refugee[1] crisis has increasingly worsened over the past decades. Specifically since 2005 there has been a severe increase of over 340% in the global refugee count. According to the UN Refugee Agency (UNHCR)[2], by the end of 2017 there were 71.4m refugees worldwide, compared to 21.1m at the end of 2005. This crisis is a major concern for governments and non-government organizations (NGOs) alike, not only from a humanitarian perspective but also from economical and geopolitical perspectives.

Recent refugee crises[3], such as the ones in Syria (6.3M), Afghanistan (2.6M), South Sudan (2.4M), Myanmar (1.2M), and Somalia (1.0M) have gained the public attention calling governments to respond. Others, such as the Guatemala Caravans[4] in which Central American refugees attempt to make their way to the US, have gained attention due to the response of the US government.

In our view, this crisis encapsulates the following key challenges:

- Difficulties in tracking and sharing refugee migration data among governments and NGOs
- Lack of valid identity documents (IDs) of refugees

There are global initiatives led by UN, such as Migration Data Portal and Global Compact for Migration[5] (GCM), and the Internal Displacement Monitoring Center[6] (IDMC). Both of these initiatives are collecting data in order to build a global database to help tackle the crisis. However, while the former is still in its very early stages[7], the latter focuses on internally displaced persons only, not on the broader definition of refugees. Still, we believe that both platforms' main hindrance is that they are both centralized systems.

We believe that a blockchain-based solution could tackle the challenges mentioned above and would provide a transparent infrastructure that governments and NGOs alike could easily adopt and share. Moreover, since the solution we present is highly modular, it could easily launch as a local initiative and then quickly develop into a global solution.

Blockchain Technology

Blockchain is a disruptive technology that combines the merits of modern cryptography and distributed ledgers. As the name suggests, a blockchain ledger consists of a chain of data blocks, sealed cryptographically and time-stamped. Each new block is a repository of the latest added data

[1] By "refugee" we refer to the UN Refugee Agency's (UNHCR) term "person of concern", which includes refugees, asylum-seekers, internally displaced persons (IDP), returnees, stateless persons and other persons of concern

[2] http://popstats.unhcr.org/en/overview

[3] https://www.mercycorps.org/articles/worlds-5-biggest-refugee-crises

[4] https://www.reuters.com/article/us-usa-immigration-caravan/second-migrant-caravan-in-guatemala-heads-toward-mexico-idUSKCN1MX2JP

[5] https://migrationdataportal.org/themes/global-compact-migration

[6] http://www.internal-displacement.org/

[7] Consultations have begun in December 2017, and since then six data bulletins were published

(in the form transactions) and is linked to the previous block. The chain propagates at predefined time intervals as new blocks are added, thus forming a chronological chain that is a trail of the underlying transactions. As the ledger is decentralized. there is no central entity that is responsible for validating transactions and updating the ledger. Each node on the network must maintain its own copy of the ledger and validate new transactions independently. New transactions are executed, *i.e.* written into a new block, only if the nodes reach a consensus on their legitimacy. The criteria for reaching consensus vary across different blockchain protocols.

Among the core features of blockchain ledgers, three are most relevant for our discussion: security, immutability and transparency.

- Security - the ledger is distributed, therefore in order to compromise the data one must hack multiple nodes at once, in order to tamper with the consensus process or implant false data retroactively[8]
- Immutability - once new data is written, approved and sealed it cannot be modified or overridden
- Transparency - anyone can access the data once it has been sealed and added to the chain

In other words, blockchain allows running a *trustless* platform, in which parties interact without having to trust one another. As long as they trust the *protocol*, they are certain that the data is valid and that they can continue interacting. This new form of interaction is a tremendous breakthrough that allows developing new solutions for old problems. For instance, digital rights management, supply chain monitoring, cross border peer-to-peer payment at a minimal fee, etc.

Biometrics Systems 101

Using biometric identifiers[9] (BI) as a distinctive and measurable characteristic of individuals is not a new concept. The Babylonians[10] and the ancient Chinese used fingerprints as a legitimate mean of signing business transactions. The first forensic use of identifying fingerprints was recorded in India in 1858. Among of the common biometric identifiers are fingerprints, face recognition, DNA, iris recognition etc. Those are all unique identifiers, therefore the most reliable means of identity authentication. BIs differ from one another in terms of their security vs convenience, and it is important to remember that none of them is considered as *the* ideal BI. Moreover, even with the most advanced technology no BI can provide a foolproof guaranteed identification of an individual. In recent years, there has been a growing use of BIs as part of issuing IDs such as passports, driving licenses, etc. In parallel, there has also been a growing concern of the consequent threat to privacy. We dwell on that later in this paper.

Biometric systems are designed to either authenticate (*i.e.* determine whether the person is who she says she is) or identify (*i.e.* determine whether the person is *not* who she says she is). Both rely on statistical matching algorithms to determine whether the BI sample

[8] Further discussion of blockchain security is beyond the scope of this paper. However, we would like to note that blockchain is considered to provide maximal data security given current available computation power
[9] While biometric identity refers to both physiological and behavioural characteristics of an individual, in this paper's context we refer only to the physical ones
[10] https://www.usmarshals.gov/usmsforkids/fingerprint_history.htm

matches an existing record. In order for an individual to be biometrically identified she must first enroll, meaning that the BIs are digitally captured and stored, on a database, a card or both. Whenever the individual's BIs are sampled again, they are compared to the available record, on the database or the card.

The largest biometric database in the world is India's national unique ID program, called Aadhaar[11]. Its vision is "To empower residents of India with a unique identity and a digital platform to authenticate anytime, anywhere". The identification process combines both BIs (fingerprints, iris and face photo) and demographic data (name, age, gender, address, etc.). As of writing these lines, over 1.2B Aadhaar IDs have been generated. While it has been the subject of vibrant discussions on privacy concerns, Paul Romer, former Chief Economist at the World Bank and winner of Nobel Prize in Economics, referred to it as "most sophisticated [system]" that he'd ever seen.[12]

Digital Identity over Blockchain

Before we discuss our suggested blockchain platform, we would like to introduce related concepts of digital identity and other existing blockchain-based ID solutions.

The most innovative concept of a digital identity is Self-Sovereign Identity (SSI). It is still under debate and there is no consensus on what it exactly is or how it will work. It suggests three types of digital identity relationships:

- Centralized - the traditional model in which the individual's identity and digital credentials are provided by the organization it interacts with, *e.g.* banks, ecommerce website, etc.
- Federated - new third party entities, called Identity Providers (IDP), are in charge of issuing digital identity and credentials, which are federated to the organizations with whom the individual interacts. Examples may be using one's social network identity to log in to other online services
- Self Sovereign Identity - full peer-to-peer relationship. Each peer controls a cryptographic wallet that stores all its IDs. With each interaction the other peer may attest the validity of the documents. For instance, when a person uploads an academic degree, it interacts with the academic institute and it cryptographically signs the transaction meaning that it attests the validity of the document. Both the document and the attestation are stored on the peers' wallets. Whenever required, the person may share the certified academic degree with any other party. Each transaction in which the information is shared and accepted serves as an additional proof for its credibility and authenticity. Another example may be proving claims such as "over 21". Upon reaching that age, the person will interact with the relevant government agency to get this confirmation based on the issued birth certificate.

[11] https://uidai.gov.in

[12] https://www.bloomberg.com/news/articles/2017-03-15/india-id-program-wins-world-bank-praise-amid-big-brother-fears

Th SSI is still at its earliest phase of formation. There are several blockchain protocols that are looking to implement it, in one way or another, such as Sovrin[13], Evernym[14] , Civic[15] and uPort[16]. All are still under development.

One of the most ambitious projects is ID2020 Alliance[17], a non-profit partnership founded by Accenture, Gavi, Microsoft and the Rockefeller Foundation in 2017. With time additional organizations and enterprises, e.g. UN International Computing Center and Mercy Crops and have joined as well. The goal is improving the lives of 1.1 billion people who live without an officially recognized identity by providing them with a digital identity. It is expected to hold personal data such as birth registration, vaccination, voting registration, refugee registration, national ID cards etc, that could be shared with NGOs, governments and enterprises. It aims to deploy a global mass-used platform by 2030. To date, it has announced two pilot projects, in Thailand and Indonesia[18], providing digital medical records for refugees and liquid petroleum gas (LPG) subsidies to locals, respectively.

Another successful project is Building Blocks by the World Food Program (WFP).[19] It was initiated in Pakistan in 2017, and later on expanded to the Za'atari and Azraq refugee camps in Jordan. As of October 2018 more than 100,000 Syrian refugees get their WFP assistance through a blockchain-based system - digital ID based on an iris scan. Since 2009 the WFP has shifted from delivering food to those who need it, to transferring them money instead. The added value is developing local economies, but the downside are the transaction fees involved, that theoretically could have been used to provide more food. Each refugee is issued with a digital wallet that stores his new identity and the funds provided by WFP. The wallet is then used at the local supermarkets to buy food. According to WFP[20], transferring funds over the blockchain saves 98% of local bank fees. This project is expected to further expand to all other WFP supported refugee camps in Jordan, hosting 500,000 Syrians.

Two smaller-scale projects are MONI[21] in Finland and BRER by Bitnation.[22] MONI is a Finnish startup collaborating with the local Immigration Service to provide unbankable asylum seekers with a prepaid debit card that also stores their digital ID. This card functions as a bank account, which they would have never been able to open, thus allows them to manage their personal finances, receive benefits from the government and even loans from other people. It even keeps a blockchain record of their credit history, which may be valuable down the road. Bitnation Refugee Emergency Response (BRER) is a more modest project, run by a Bitnation, a decentralized non-government Bitnation organization. The project seeks to authenticate and issue Blockchain Emergency IDs (BEID) to refugees, providing them with the most essential blockchain-based proof-of-existence.

[13] https://sovrin.org/
[14] https://www.evernym.com/
[15] https://www.civic.com/
[16] https://www.uport.me/
[17] https://id2020.org/
[18] https://www.prnewswire.com/news-releases/id2020-alliance-launches-inaugural-pilots-welcomes-new-partners-at-annual-summit-300713089.html
[19] https://innovation.wfp.org/project/building-blocks
[20] https://unite.un.org/sites/unite.un.org/files/session_2_wfp_building_blocks_20170816_final.pdf
[21] https://www.technologyreview.com/s/608764/how-blockchain-is-kickstarting-the-financial-lives-of-refugees/
[22] https://refugees.bitnation.co/

The project has not been recognized by any official organization and there are no further details about its adoption.

Suggested Solution

We propose a blockchain-based solution that solves the identity problem immediately, as we regard this to be the crux of the matter. On the refugee side, with a new official identity, the refugee is instantly and officially recognized by an asylum state. From the receiving state's perspective, identifying refugees on arrival allows for better monitoring and data sharing as part of a multinational effort for coordinating humanitarian assistance. Additional features, e.g. digital wallets, can be added rather simply to the platform down the road.

The platform will be deployed as a permissioned blockchain, meaning that there are certain restrictions on joining as a node and accessing data. Naturally, this is due to privacy matters. The nodes may be national immigration services, border checkpoints or aid organizations. They will be the ones that carry out the enrollment and identification process, including writing new identities on the blockchain as a proof of registration and authentication. The nodes are also users on the blockchain, meaning that they interact with the refugee in form of transactions.

So, whenever a person enters a border checkpoint and self declares to be a refugee, the process will be the following:

1. **Enrollment** - regardless of whether the person obtains an official ID or not, she enrolls in the biometric identity platform, *i.e.* a new biometric ID is generated on the spot along with a cryptographic wallet. This wallet stores the new ID and all other relevant metadata, e.g. location, time, additional documents provided by the refugee, relatives etc.
2. **Identification** - once the biometric ID is available, the checkpoint tries to identify the individual, to verify whether there are no other matching IDs on the ledger
3. **Data transmission** - the individual makes his first transaction on the blockchain, in which she sends all that info to the checkpoint. The data is encrypted so that only both sides can read it. All other nodes will only be able to verify that there has been a transaction between user X to node Y at time Z. They know where node Y is located, and they are able to extract from this transaction the cryptographic digest[23] of the biometric identity. This allows them to look for a match when they generate a new biometric identity for a refugee

Once all three steps are done, the refugee may be referred to the next steps of the "standard" procedure, according to the receiving state's immigration policy

There are many benefits to this platform, stemming from core features of blockchain, as discussed earlier:

- Efficient end-to-end process
- Refugees get a new immutable digital ID proving their existence and documenting their asylum request

[23] A digest is the output of a cryptographic hash function. In a nutshell, those are one-to-one mathematical functions that stand at the base of modern cryptography. Further discussion is beyond the scope of this paper

- Multi-purpose new ID with an immediate use and additional uses down the road, e.g. cryptographic wallet
- Secure platform providing refugees with maximal level of privacy
- Information is easily shared ***only*** among nodes on border checkpoints and humanitarian aid organizations. Therefore, in special situations, e.g. locating lost family members, the process is fast, simple and easy location of lost family members at the receiving state
- Each checkpoint can easily track the amount of refugees it has assisted. In that manner, national immigration services can easily aggregate accurate data from all checkpoints, in real-time
- Receiving states and aid organizations can better track and monitor refugees influx and improve cooperation

Still, there are certain challenges involved with this platform. The main challenge doesn't concern blockchain directly, but it is inherent to all biometric identity systems. As close as biometric identifiers get, they are still not completely foolproof and rely on *statistical* algorithms, therefore a certain level of identification errors is inevitable. We consider this as a technical challenge that can and should be resolved by the biometric identification equipment provider. Moreover, this technology is developing fast and the platform keep getting more sophisticated and accurate. In our context, there can be multiple layers of generating the new identity, that do not rely only on BIs, as discussed earlier. Another major challenge is user privacy. In our view, blockchain is the optimal solution to tackle that and further discussed in the next section.

Privacy Concerns

Privacy is a major pain point in any platform that manages and holds user data. Any centralized database is prone to hacking and data leakage. Let us examine several aspects of this concern and how we think they can be mitigated.

The most basic feature of this platform concerns access level to individuals' private data. In our view it is only reasonable that once an individual arrives at a checkpoint asking for asylum, that checkpoint (and the immigration service that it represents) is entitled to maintain full access to her personal data. Furthermore, in order to provide the refugee the opportunity for a fresh start at the receiving state, it *has* to hold her biometric identifying data, as it does for its residents. Still, checkpoints from other countries are most definitely not entitled to access that data, for privacy considerations. They will only gain access to the "public" data, *i.e.* individuals' arrival at different checkpoint (nodes) at certain times. Modern cryptography is fully capable of providing this kind of data access differentiation.

The major threat is defending the platform from being hacked and stealing sensitive data. Blockchain introduces a new concept for improving overall data security through modern cryptography and decentralization. It is arguably the most secure platform there currently is, that allows multiple parties to interact efficiently. In order to hack it, it would require hacking multiple nodes at once as mentioned above. Furthermore, there are two level of security on our platform - network security and transaction security. The network security is covered by the type of the

network, which is a permissioned blockchain, while the transaction security is covered by the blockchain protocol, *i.e.* the data encryption.

Our suggested platform will run over a permissioned blockchain, in which nodes must be approved prior to joining the network. Only government agencies or recognized aid organizations could become nodes, thus making sure that the private information does not fall into the wrong hands. On the transaction level, the data is encrypted and can only be accessed using a private key, which is held by the individual only. This means that nodes have full info, only on the transactions (*i.e.* refugees) that they were part of. This means that each checkpoint does not know the identities of refugees who went through a neighboring checkpoint, they only know that they were there. This solution prevents data breaches, as even if someone manages to imposter as a legitimate node, all he gets access to is a ledger of encrypted transactions. The data is encrypted by so many different entities, each has access only to small portion of it. In certain cryptocurrency blockchain networks, people may hold substantial amounts of cryptocurrencies, making it worthwhile to try to hack their wallet. While our platform it seems that no one would actually be interested in hacking a specific wallet, as there is no reward involved.

Summary

The data shows that the influx of global refugees is worsening as time goes by. Moreover, as unfortunate as it may be, it seems that this problem will never be fully resolved, and that there will always be those who are forced to leave their homes, under tragic consequences, to seek shelter somewhere else.

Of all the potential positives that blockchain can enable we find that improving the efficiency of government-related services is among the most prominent. A blockchain-based global database could be a forward thinking and innovative approach towards helping the global effort for solving the refugee crisis. It has great potential to aid multiple governments, while also making the day to day lives of documented and undocumented refugees logistically more comfortable. Furthermore, we believe that this platform can be a key strategic element to solving a global humanitarian problem and improving the lives of the weakest individuals in our society.

Who We Are

Hexa Foundation is an not-for-profit organization focused on using blockchain to create social impact. The organization was co-founded by Netta Korin, who comes to the Foundation following years of experience in business, government and non-profit industries. Most recently, Netta worked as a Senior Advisor in the Israeli Ministry of Defense to General Yoav (Poly) Mordechai, Head of CoGAT, and has an in-depth knowledge of the socioeconomic problems in the Gaza Strip. Prior to that position, Netta worked as a Senior Advisor to Deputy Minister Dr. Michael Oren in the Prime Minister's Office in Israel, focusing on Palestinian issues. Netta has held board positions in several non profit foundations in both Israel and the United States.

The Hexa Foundation is part of the Orbs Group. Both were created by the founders of Orbs, a blockchain platform for consumer applications. Orbs Group is the largest group dealing in blockchain solutions in Israel, with close to 60 employees focused on the blockchain field. The Hexa Foundation aims to use blockchain for social impact and harness the mind power of our ecosystem and network to help solve the region's and the world's most pressing humanitarian problems.

For more information please contact Netta Korin (netta@hexa.org)