Spring 2023
CIS 8393: Topics in Digital Innovation

Securus: Using blockchain to detect and mitigate human trafficking

Team Members:
Adedayo, Grace
David, Denise
Marthi, Prathibha
Norwood, CJ
Pierre-Louis, Kayla

Securus: Using blockchain to detect and mitigate human trafficking

1. **Introduction**

A peer-to-peer missing persons' framework for local law enforcement and mass transportation hubs (airports, train stations, bus stations, border stations) that would assist law enforcement in preventing cross-country state travel of human trafficking victims. Once victims are trafficked across state/country borders, it makes it more challenging for authorities to track down the victims. Depending on how advanced the trafficking organization is, victims can be given false IDs and passports, preventing transport facilities from receiving a notification once the victim's alias is inputted. Securus will utilize facial recognition technology (FRT) to scan travelers; these facial scans will be cross-referenced with all missing person notices submitted to the framework by government authorities. If a traveler is a 99.5% or more match to a missing person in the database; the traveler and their party will be separated and held for questioning by the local police. The percentage was decided based on current AI-powered facial recognition models[1]. The database of missing person information will utilize a peer-to-peer framework; with local authorities being the only ones to upload missing person data and local transport facilities receiving the updates to the database for traveler FRT scans.

The U.S. Department of State defines "human trafficking" as a crime whereby traffickers exploit and profit at the expense of adults or children by compelling them to perform labor or engage in commercial sex. The Global Estimates of Modern Slavery report (released in September 2022) estimates that there are 27.5 million people in situations of modern slavery on any given day[2]. The U.S. Department of State estimates that 14,500 to 17,500 people are trafficked into the United States each year. People of color and immigrants are disproportionately victimized by this heinous exploitative industry[3]. Please note that due to the hidden nature of the crime, data and statistics may not reflect the full nature or scope of the problem. This unlawful industry is a worldwide crisis and due to advancements in technology and strategy, the nature of these crime syndicates has become more difficult for authorities to contend with. When a trafficking victim is relocated to another state or country it makes it even more difficult for authorities to rescue and track down the victims. The Securus blockchain solution will prevent the transport of trafficking victims by cross-referencing the facial scans of all travelers with the missing persons' database.

2. **Blockchain Application Framework**

Securus notes the security of biometrics data as its main priority. Even though the speed of processing takes a secondary seat, timely transactions are still an important component of the blockchain solution. With this, the Blockchain Application Framework is as follows:

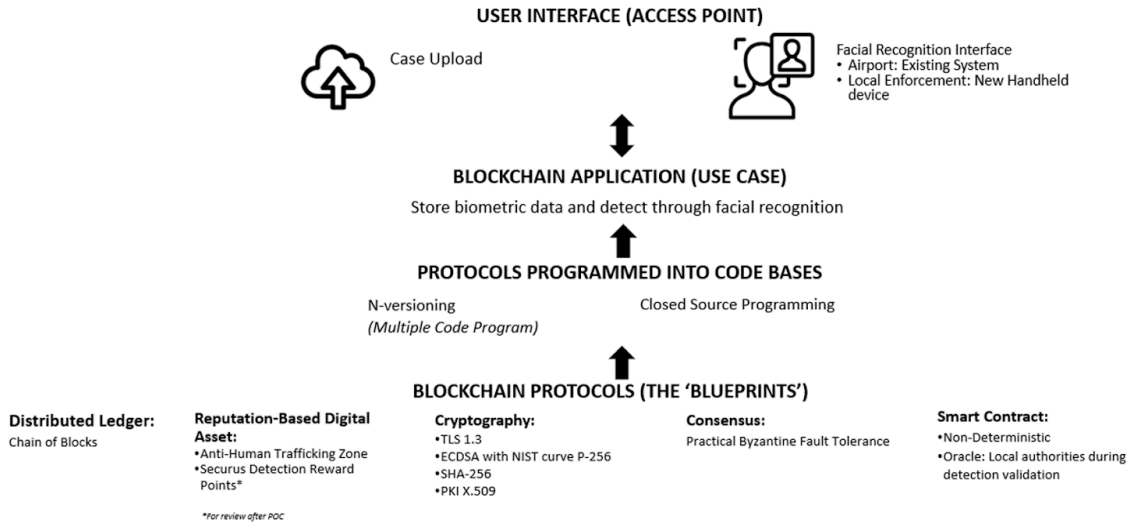


Photo Reference: https://thenounproject.com/

1. Blockchain Protocols

1. Distributed Ledger

Securus will utilize a chain of blocks structure for its distributed ledger. A block will contain a header referencing the previous set of blocks of transactions, and a set of sequence transactions. Transactions that are recently approved are sequenced and stored in the block. These blocks form a chain of sequenced blocks as more transactions are added, all the way back to the genesis block (the first block created).

Securus transactions are not as complex since it will reference and update the status of the biometrics of the missing person. Moreover, a chain of blocks structure has one of the best securities among the other types of distributed ledgers in which the system has it as its main priority.

2. Native Digital Asset

Securus compensates participants using reputation as a type of digital business asset class. The purpose of this type of digital business asset is to promote usage by rewarding

participants through prestige or influence in acquiring the asset after a successful detection and retrieval of the victim of human trafficking.

The organizations (such as airports, government agencies, and localities), are provided with a reputation type of digital asset in the form of a certification in the Anti-Human Trafficking Zone. These digital assets function as a marketing tool for the public to see that the area is safe from human trafficking.

As for the local law enforcement, they are provided with Securus Detection Reward points. This is an incentive-based program wherein points are gained during the successful detection and resolution of illegally trafficked persons. This is used as part of their performance metrics and potentially can lead to special bonuses. This will be available in the initial run of Securus to promote system usage, but it will be reviewed once the system proof of concept has been passed and expanded to other states, borders, or countries.

3. Cryptography

Securus's cryptography follows Hyperledger Fabric's cryptography[4]. Securus utilizes:

- Network level node security and authentication: TLS 1.3

The goal of this node is to prevent unauthorized access to the network. TLS (Transport Layer Security) utilizes symmetric cryptography to encrypt the transmitted data. The keys are uniquely generated for every connection and are based on the TLS handshake. The latest version of TLS is 1.3, wherein it is designed to address the pitfalls of TLS 1.2, leading it to be faster and more secure[5].

- Client and node signatures: ECDSA with NIST curve P-256

ECDSA or Elliptic Curve Digital Signature Algorithm will be used as the cryptography encryption algorithm for the client and node signatures. According to Adalier, Mehmet and Teknik, Antara in their research on this type of cryptography[6], ECDSA P-256, a prime curve that has been used extensively in critical infrastructure projects, is also being used as the Elliptical Curve Digital Signature Algorithm for AS-path signing and verification in the BGPSEC protocol. ECDSA P-256 is known to be efficient in terms of performance.

- Hash Function Algorithm: SHA-256

SHA-256 algorithm is the commonly used hashing algorithm for cryptography. This algorithm satisfies the five main properties of an ideal cryptographic hash function. One of them is being collision resistant - computationally infeasible to have two different

messages with the same hash value but at the same time, the same message results in the same hash value[7].

- Client and node authentication: PKI X.509

The public key infrastructure (PKI) will be used to authenticate clients and nodes. This is currently the most popular system for security management[8], especially, since Securus will be utilizing existing infrastructures of the government legacy systems on its proof of concept. X.509 will be used as the format for the PKI certificate, which is based on the widely accepted standard[9]. The two main benefits of using this type of authentication are that it is widely trusted by organizations in the digital world and that it is scalable for future Securus applications.

4. Consensus

Due to the confidentiality of the data being stored and utilized, Securus requires node users to be known and centralized. Data stored are highly private and confidential given the cases that it might be linked with.

During its blockchain system design phase for the consensus algorithm, one of the requirements considered is looking into the long-term implementation of Securus which would need to cater to multiple users-transactions being processed at any given point in time. Given a load of simultaneous transactions being processed, speed and optimal resource consumption should be considered. Aside from Securus aiming for security and speed, the system is designed to be as eco-friendly as possible in its use of resources.
Practical Byzantine Fault Tolerance (PBFT) is the optimal consensus algorithm that Securus will use. It has the best confidentiality, users are known, highest transaction per second, and has the lowest resource consumption.

For future versions, Securus will need to consider renewable energy resources to run its algorithm.

5. Smart Contracts

Smart contracts for Securus will be written as non-deterministic on transactions that require closure after detection. Facial recognition technology as of this writing is being trained to improve its accuracy, therefore, would require human intervention after detection. Local authorities may need to validate the potential missing person outside of Securus, and once a resolution has been created (either found, resulting in the closure of the case, or wrong detection, leading to the case being kept open).

2. Protocols Programmed into Code Bases

Securus will be utilizing the Hyperledger Fabric as its basic blockchain protocol, however, there will be modifications to retrofit the government's requirements. It utilizes a variety of programming languages for most of its components to add a layer of security to the blockchain system. Unlike most blockchain code bases, the Securus code base will remain private (closed source) since this will be treated as a national security concern. The data stored and referenced in the system are treated as highly confidential. To keep the public trust, this blockchain will provide privacy and confidentiality standards for the public to read.

3. Blockchain Application

Securus' use case is a store and detects application, utilizing government-deployed devices. It is used to store case data information, specifically missing person biometric data; in the case of minors, parents have the option to provide their biometric data along with the child. This can assist with facial detection accuracy as a second point of validation. This information is then referenced by the facial recognition AI during the scanning and detection of airport personnel or ground local law enforcement.

4. User Interface

There are two main points of access for Securus which are for case uploads and for facial recognition detection. Most of this blockchain system will reside in the backend of the existing government systems.

Case uploaded access point is used by law enforcement to upload the biometric data into the blockchain system. In the initial phase, the system will capture the login credentials of the existing legacy system (software and hardware) used by law enforcement to open the application wherein they file the missing person. Next, Securus will capture the biometric data provided by the case reporter - either the missing person only or including the immediate family biometric data, if provided.

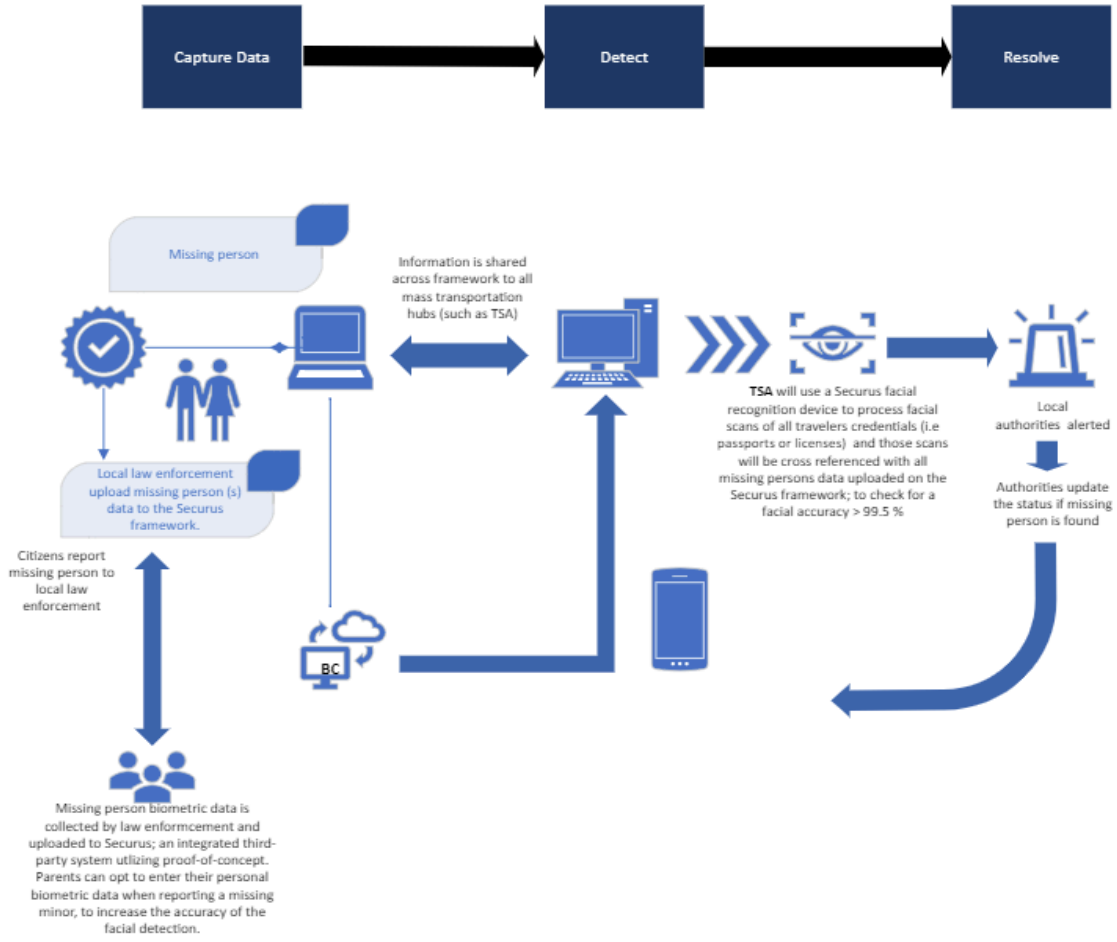
Facial recognition detection access point is broken down into 2 sub-systems depending on the user: the airport personnel, and the local law enforcement. For the airport personnel, like the case upload access point, Securus will utilize the existing software and hardware where the airport personnel log in during their shift and use the device to scan and validate the identification provided by the passenger. The blockchain system will capture both user credential login and scanned biometric data. The scanned biometric data

will then be cross validated within Securus if the profile of the passenger exists. The target transaction time for this process should be less than one second per scanned passenger, to minimize the impact of regular airport validation operations. Once detected as a potential active case, the airport personnel will ask the passenger to step aside for further questioning and validation. A resolution will be provided within Securus - if the case is still tagged as open or resolved, meaning the detected passenger was identified as the missing person.

For the local enforcement, a device will be provided wherein they would need to log in using their credentials during their shift, to be used to scan the potential area traveled by the missing person. Like the integrated airport system, once there is a detected potential active case like the actual person in the scanned area, the local law enforcement will perform further validation with the potential missing person. The resolution method will be provided into the handheld device like the airport personnel - if the case is still tagged as open or resolved after validation.

Digital assets are rewarded and paired with the user credentials once the missing person case is resolved after validation.

3. **Blockchain Solution**



The model above shows the high-level process flow of the Securus blockchain; it is subjected to revision as Securus becomes more accepted across more law enforcement agencies.

4. GOVERNANCE MODELS

1. Governance Model

Securus will follow a glide path for its governance model. This is to ensure the model will be efficient and effective from proof-of-concept until rollout. In its initial stages, Securus will utilize an oligarchy governance model, with the intention of progressing towards a representative meritocracy as the deployment of the application scales into a wide range of networks.

1. Oligarchy

   Oligarchy is the preferred starting point for Securus. The starting point of Securus will be composed of the founding partners. This creates an efficient model when making decisions and executing of the changes during the initial phases of the project. This model also provides clear control and accountability, which is crucial during its proof-of-concept and moving forward to roll out. The governance model will change once it had served its initial purpose, and moves forward to include more localities, states, etc.

2. Representative Meritocracy

   Representative meritocracy is the endpoint goal of governance for Securus. This ensures the sustainability of the program long-term through the inclusion of eligible parties based on merit to be included in the governance of Securus. Merit will be based on a multitude of factors such as, but not limited to, contribution to the closure of human trafficking cases, and level of participation with the system. It is important to give accountabilities in decision-making, program execution, and future upgrades to encourage better participation.

2. Vision and Mission

1. Our Vision

   To build a trusted and secure network that mitigates the spread of human trafficking and the exploitation of people through unlawful transportation using blockchain and AI technologies.

2. Our Mission

   - To further mitigate human trafficking and the exploitation of people through unlawful transportation.
   - To build a trusted and secure network that mitigates the spread of human trafficking; the exploitation of a person for labor, services, or sex.
   - To assist with identifying trafficking victims through the use of blockchain and facial recognition technologies.

3. Funding Model

   Securus will initially be funded by an angel investor/s to kick off the project's development phase. Target angel investors will be similar to Bill and Melinda Gates Foundation or agencies that are passionate about mitigating human trafficking such as The Polaris Project. The angel investor will be given a 33% stake in the company's equity share.

Securus will then be pitched to Federal Reserve System (FED) to get an NHS (National Health Service) contract to help fund the operation scale-up.

A step up to funding Securus would be through Security Token Offering (STO). STO follows legal compliance and licensed ICO. This provides anti-fraud security for investors.

In the US, DOT (Department of Transportation) awarded $5.4 million in transit grants through the Federal Transit Administration to address public safety issues, including human trafficking, and over $3 million in grants through the Federal Motor Carrier Safety Administration to support state counter-trafficking efforts through driver's license standards and programs[10]. Given that Securus aligns with one of the issues DOT aims to address, this government agency will be considered a viable partner to fund the operations.

Once the system has been launched and had been widely accepted, it will change the funding model to be incorporated into the transportation tax. This will be an add-on of 0.5% - 1% on the existing transportation tax model, treated as a processing fee, similar to the processing fees of any current cloud-based system. The pricing model will be further computed depending on the resources used by the system, future system improvements, and other operational expenses to maintain Securus.

4. Rights of Participation and Validation

Securus is considered the top priority of Securus, hence, it will strictly follow a private-permissioned blockchain. Participating law enforcement is the only one who will have access to and perform transactions within the system. This will also help preserve the confidentiality of the system. It will strictly comply with the regulations regarding the handling of its data, points of participation, and validation. When the network of users expands, the system will need to consider in its pipeline the governing rules on data protection and privacy.

This system follows a subscription-based model as part of its deployment plan. Given this, if the agency decides to opt from Securus, its rights to participate and validate will be revoked.

5. Right to Override

Securus follows the hierarchy of law enforcement within the country in it had been implemented. To be specific, in the USA, the law enforcement agency that submitted the notice to the blockchain application and the missing person case is taken over by another

jurisdiction, for example, federal or state law enforcement, this would result in the commandeering agency would obtain override rights from the initial law enforcement agency that uploaded the missing person notice.

6. Governance Residence

Securus will perform on-chain operations mostly as its governance residence. The decisions will be based on the implementing country's law enforcement hierarchy. As an example, in the US, this will follow as local/city, going up to state and then federal. This ensures that any decisions made within the system are based on the country's standards and will not deviate from any law or regulations.

If there ever is a disagreement about governance residence specifically around jurisdiction rights on human trafficking cases among government law enforcement, this will be handled off-chain. Off-chain governance decisions will be based on whatever the outcome of a jurisdiction dispute is.

5. **Ethical Design**

1. Promotion of Human Values & Environmental Sustainability

Securus works to mitigate human trafficking and provide safer environments for mass transportation. As commercial travel becomes more accessible to people globally, it is critical to ensure that airports and mass transportation hubs increase security measures to control the means by which these trafficking systems could be manipulated to exploit victims. Each transportation hub where Securus has been successfully deployed to identify and intercept the trafficking of a missing person will be certified as an Anti-Human Trafficking Zone to publicize to travelers that this particular hub has well-established safety precautions to protect travelers.

2. Privacy and minimum disclosure

As an additional measure of data protection and privacy, the data sources will be exclusive to government owned missing persons reports. Government law enforcement agencies will upload missing person notices/possible trafficking victim notices to the Securus blockchain application, so the application is semi-automating existing practices and adding technology enhancements to increase efficiency. Travel organizations such as airports, bus/train stations and border patrol stops will all have their identification databases linked to the block chain, and only the government law enforcement personnel staffed at these locations will have access to the application on approved devices. Therefore, Securus serves to modernize security protocols by partially automating and

enhancing existing practices. As changes in privacy laws occur new smart contracts will be created to address the new requirements.

3. User Control and Agency

Since Securus is a private and permissioned application, this governing council will ensure the enforcement of data privacy and security in the way Securus manages all collected data.

4. Voluntary participation

Securus is an application that offers an alternative and additional travel security tool to governmental law enforcement organizations around the world, so participation is exclusive to those law enforcement and government agencies that apply their discretion in utilizing the tool to help manage travel security protocols in mass transportation systems. Although it cannot exclusively eradicate every method by which human trafficking occurs, its effectiveness increases as more agencies and countries join its network and use it as a resource.

5. Equity, Fairness, Inclusion, and Non-Discrimination

Human trafficking is a global pandemic, but disproportionately impacts disenfranchised communities of color and more specifically, women of color. Therefore, five graduate students comprised of 4 women of color and 1 man of color from 4 different countries decided to take a call to action and created Securus. By merging our individual unique cultural experiences and concerns we believe we have developed a healthy security framework that will better serve targeted people and support law enforcement agencies globally.

6. Safety and Security

Security is paramount for Securus to operate as intended, so it will be most beneficial for the rights of validation for the application to remain private and permissioned and for the rights of participation to remain exclusively with government law enforcement personnel to track all access and interactions along the process. We do observe that facial recognition technology historically presents challenges when it is solely based on a predominant societal phenome. However, since the founding board for Securus was comprised of five different people of color from four different countries the application was able to pool data from all various countries to create a more comprehensive and inclusive facial recognition model it will deploy. We do observe that there will be learning opportunities for the model where mistaken identity might occur, but these occurrences will help create more skilled updates to improve the model.

7. Transparency and Explainability

   Securus uses public missing person data sourced from governmental law enforcement agencies, so data lineage remains transparent. Our governing body made up of representatives from each participating governmental law enforcement will work to ensure that the smart contracts and FRT model continue to work to become more comprehensive and integral. Additionally, privacy, confidentiality, and success statistics will be made available to the public to evidence the tool's effectiveness.

8. Potability and Interoperability

   Since Securus is an alternative security enhancement tool that governments can willingly choose to join or opt out of their subscription to the application, they will not be locked in and maintain their rights to not participate.

9. Professional Responsibility
10.

    Securus was formulated to promote responsible oversight in travel security for governments and law enforcement agencies, and this is exhibited throughout the blockchain's design and governance structure. Consequently, continuous improvement in future versions will be achieved by collecting feedback and implementing changes from governing policies.

6. **Emerging Trends/ Technologies/ Rises**

With a new era of technology on the rise, it is no surprise that these technological advancements have been utilized within the crime control industry. Emerging technologies in artificial intelligence, facial recognition, and blockchain are a few of the tech solutions on the rise in this government industry[11]. As crime syndicates have engaged in emerging technologies; governments need to do the same, to regulate and eradicate these complex forms of malfeasance. Facial recognition technology (also referred to as FRT) is becoming a critical component for crime control in the United States; from identifying human trafficking victims to suspected murderers; advancements in this technology, though substantial, have been highly unregulated. The lack of regulation and standard policies in the application of this technology has spurred moral and ethical debates. A study conducted by the Bureau of Justice Statistics, FBI Uniform Crime Report, and the U.S. Census Bureau found that law enforcement FRT use facilitated greater racial disparity in arrests. *"This relationship was underpinned by statistically meaningful and positive FRT effects on Black arrest rates and negative effects on White rates*"

Johnson, Thaddeus L., et al. “Facial Recognition Systems in Policing and Racial Disparities in Arrests[1][2].

Essentially the study found that there was less accuracy when deciphering black bystanders compared to their white counterparts aiding in the positive increase in Black arrest rates. The study also revealed that even though FRT may appear objective in nature; this technology can become problematic if racial and ethnic biases get encoded in the software. Various studies around the world have found the FRT is only as good as the data inputted; so, if dynamic data is encoded for one racial group and not another, the facial recognition technology can have a harder time deciphering facial characteristics in the racial group that had non-dynamic data inputted. This scenario can be seen in homogenous countries; FRT in countries of people with darker skin tones, have better accuracy when identifying darker persons compared to lighter ones. From a security and risk perspective, it is very important to have diverse and dynamic data encoded in FRT software development; especially when the FRT will be used in western countries with diverse populations. In addition to incorporating the diversity of facial data, quality assurance testing is necessary to make sure the FRT has reached the 99.5% accuracy rate before deploying it to the Securus blockchain solution.

As FRT evolves the hardware options have become more versatile; there are many handheld biometric solutions. Handheld options can prove beneficial for the Securus blockchain application as it can prove more attainable for mass transportation entities (i.e. bus stations & train stations) that may find more sizable FRT hardware unaffordable.

Lastly, though the Securus blockchain solution should only be used for the purpose of locating human trafficking victims; there is a possibility that local authorities will attempt to upload alleged offenders. Law enforcement can attempt to misuse this application to track down alleged assailants deviating from the application's initial purpose. Security policies should be strict, to avoid liability in civil lawsuits if ever a law enforcement agency wrongly apprehends or prosecutes an individual using the Securus application. The Securus blockchain solution should exclusively be seen as a solution to prevent the relocation of human trafficking victims at mass transportation hubs rather than a technology to track down and locate victims.

7. **Bibliography**

[1] "Face Recognition Accuracy : How Accurate Is AI Powered Face Recognition." *Hyperverge*, 16 June 2022, www.hyperverge.co/blog/accuracy-of-ai-powered-face-recognition. Accessed Feb. 2023.

[2] "About Human Trafficking." *U.S. Department of State,* https://www.state.gov/humantrafficking-about-human-trafficking/#human_trafficking_U_S. Accessed February 2023.

[3] "U.S. Immigration Policy and Human Trafficking: Two Sides of the Same Coin." *Human Trafficking Institute,* 11 August 2022, https://traffickinginstitute.org/u-s-immigration-policy-and-human-trafficking-two-sides-of-the-same-coin/#:~:text=The%20U.S.%20Department%20of%20State,the%20United%20States%20each%20year.&text=An%20estimated%2072%25%20of%20these%20victims%20are%20immigrants. Accessed February 2023.

[4] "How is Hyperledger fabric security?" *Stackoverflow,* 16 December 2020, https://stackoverflow.com/questions/65326298/how-is-hyperledger-fabric-security. Accessed February 2023.

[5] "An Overview of TLS 1.3 – Faster and More Secure." *Kinsta,* 5 May 2022, https://kinsta.com/blog/tls-1-3/. Accessed February 2023.

[6] Adalier, Mehmet, and Antara Teknik. "Efficient and secure elliptic curve cryptography implementation of curve p-256." *Workshop on elliptic curve cryptography standards*. Vol. 66. No. 446. 2015.

[7] "The beautiful hash algorithm." *Ellis, Steven,* 2018 December 13, https://steviecellis.medium.com/the-beautiful-hash-algorithm-f18d9d2b84fb#:~:text=It%20is%20collision%20resistant%2C%20meaning,in%20the%20resulting%20hash%20value. Accessed February 2023.

[8] "Authentication: How does PKI-Based Authentication Work?" *Axiad,* 2022 February 3, https://www.axiad.com/blog/pki-based-authentication/#:~:text=Two%20of%20the%20major%20alternatives,based%20cryptography%20and%20certificateless%20cryptography. Accessed February 2023.

[9] "What is an X.509 Certificate & How does it work?" *Sectigo,* 2021 January 7, https://sectigo.com/resource-library/what-is-x509-certificate. Accessed February 2023.

[10] "Human Trafficking: Transportation Leaders against Human Trafficking." *U.S. Department of Transportation.* Accessed February 2023.

[11] "How Technology is helping to stop human trafficking." *Covenant Rescue Group,* 2022. Accessed February 2023.

[12] Johnson, Thaddeus L., et al. "Facial Recognition Systems in Policing and Racial Disparities in Arrests." *Government Information Quarterly*, vol. 39, no. 4, Elsevier BV, Oct. 2022, p. 101753. https://doi.org/10.1016/j.giq.2022.101753.