Problem: Refugees do not own their own identity

The Internet is becoming an integral part of our everyday existence in practically every sector as it spreads throughout the globe. The Internet is a digital, transnational, exponential, and technology network that is not constrained by physical boundaries. The transition from paper to electronic computing, as well as Internet 1.0[1] and 2.0[2], were among the most significant transformations in contemporary history. Digitalization, computation, and the Internet have affected practically everything today. Many believe that blockchain development will allow a new era of Internet 3.0[3] to be established.

Despite advancements and disruption in other fields, the identification systems we use today are paper-based, nationally-driven government identity systems that do not take advantage of Web 3.0's capability. Due to a lack of contemporary technological infrastructure, millions of individuals rely on — or are excluded from — identity systems. When it comes to refugees, the problem is made worse because most of them leave their valuables and national identity cards behind when they flee their country[4].

Most identity systems are developed and administered from a single location, do not connect or link to other platforms, and do not provide the identity owner a sense of entitlement or authority. These systems have resulted in inefficiencies, data theft, threats, breach of information, and identity fraud, leaving billions without any type of financial account[5].

Many centralized identity management solutions have significant security flaws[6]. The recent Adobe Inc data breach, which may have exposed the personal information of up to 7.5 million people, underscores the fragility of centralized databases and puts into question the policy of collecting massive centralized sets of extremely sensitive data[7]. Citizens of whole countries (such as Sweden[8]) have been affected in some cases by potentially fatal personal data breaches. These breaches are frequently the consequence of insufficient precautions in place to prevent unauthorized access to data, rather than hacking or other intentional attempts. Moreover, since people do not own their data, private organizations such as Facebook, Google etc. collect, store and sell user's personal data without their consent such as the Facebook-Cambridge Analytica scandal.[9]

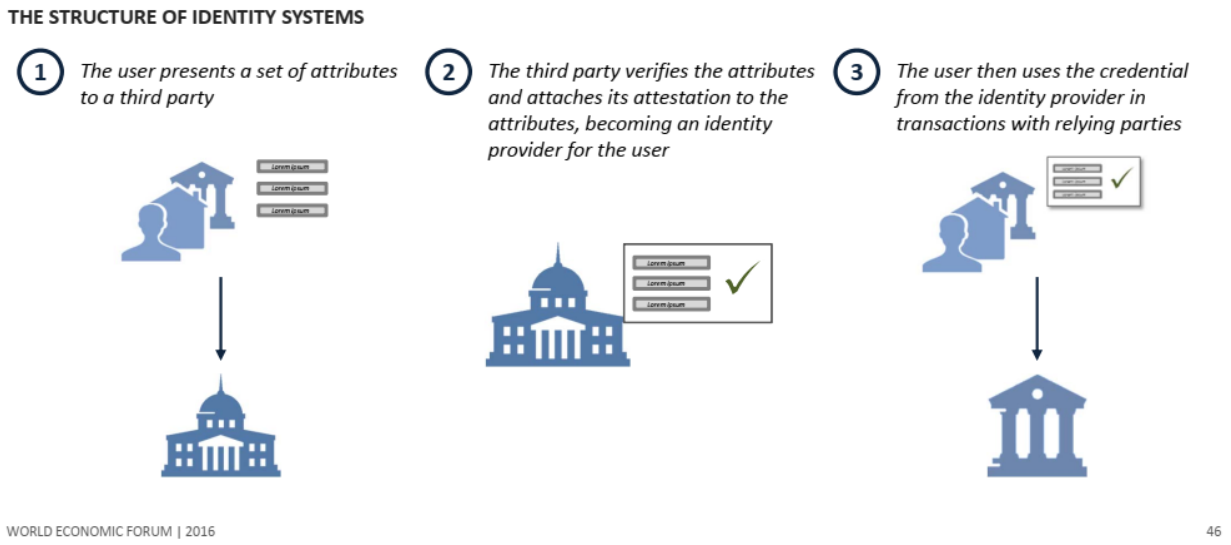
Current refugee identity systems have mostly failed to provide identity owners with any of the most fundamental needs for a successful identity system, including security, privacy, ownership, access, protection, interoperability, or linked data transfer.

Traditional centralized identification systems have several flaws. The establishment of a sustainable digital identification paradigm for our growing global society is increasingly critical to ensuring that refugees retain ownership of their identities.

Background

Entities in an Identity Transaction

An identity transaction normally involves three parties: an identity owner **(IO)** (a refugee in this scenario), an identity claim issuer **(CI)** or third party (such as a notary public or justice of the peace), and a reliant party **(RP)** (such as a bank or other financial institution). One or more identification claims **(IC)** are present in the **IO** (for example, "My name is Rahim Chowdhury" or "I was born on April 7, 1985"). The **IO** can then share these verified claims with a relying party to acquire access to the relying party's products and services, such as opening a bank account or renting houses.



For example, a refugee **(IO)** may wish to demonstrate to a currency exchange **(RP)** that they are a Myanmar citizen (claim), that they own a Myanmar passport (evidence), and that the electronic copy they are giving is a certified genuine copy of the original. This is an electronic identification claim that has been confirmed after receiving attestation from a notary. The future of digital identification is verified claims.

All of these stakeholders are frustrated by the present paper-based, centralized identity systems and would profit from a digital, decentralized approach. Moreover, many refugees do not even have the paper-based proper identification document required by these institutions and fail to verify them.

Limitations of a centrally managed refugee identity system

Security and other threats

Most identification systems have massive centralized databases with millions (or billions) of records. These centralized databases are valuable targets for hackers because of their sheer scale. They are quite easy to steal and exploit.[10] Because the payoff for a successful breach grows exponentially with the number of identities in the database, as the database becomes larger, it becomes more vulnerable to attack. Furthermore, a single huge database (as opposed to many, segmented, decentralized databases) is frequently associated with a single point of failure.

Typically, centralized identity systems are maintained by a single governing body, which then employs third-party processors to get access to databases and process data, frequently without enough controls or supervision, making the databases even more vulnerable to data breaches. A centralized identification system is susceptible to third-parties with authorized access, even if the operator is trustworthy. Individual identification documents are highly valued commodities that may be easily sold on the black market. Criminals who buy stolen identity data can use it to conduct fraud and other crimes in the identities of innocent people. Beyond the apparent harm that identity theft causes to the identity owner, such breaches expose the central database operator to serious liability.

Restricted Access

The operator restricts access to the data to try to prevent illegal access to these centralized databases. However, identity owners are frequently denied access to their own data as a result of this.[11] If operators refuse to provide access to the data, it cannot be connected to the identity owner's advantage. Connected data is an important aspect of digital identification since it allows the identity owner to construct linked patterns in data to their advantage. Linking data is not a technologically difficult task as these technologies are easily available today[12].

This is exacerbated by the fact that the refugees must go through a lot of trouble to modify their personal information, and with government delays and inefficiencies in the existing system, this is completely unfavorable and extremely costly.

URIs (a technique to identify entities), HTTP (a basic but universal mechanism for obtaining resources), and RDF (a general graph-based data model for structuring and linking data)[13] are all key technologies that facilitate linked data. Individual identity owners cannot benefit from connected data despite the fact that these technologies have been present for years.

In addition to the technological limits and security dangers associated with employing a centralized database, a single major database operator of identification data has a number of commercial problems.

Data Security Compliance

A huge, globally centralized identification database might also violate data privacy and security rules.

National and international data protection regulations are intended to guarantee that data controllers implement policies and processes to keep personal data as safe as possible, with the possibility of severe monetary penalties and possibly jail if they do not. However, each jurisdiction's regulations are unique, and compliance criteria vary greatly. In recent years, there has been a growing tendency across authorities to implement data export regulations. This creates a barrier to entry for new businesses who are unable to fulfill these onerous and very costly compliance standards.

The idea of user permission is central to most data protection legislation. Refugees usually offer this when they provide their personal data through biometrics scanning. The refugees cannot readily grant (or revoke) consent or track the consent they give over time because they are not at the core of present identity management processes, despite the fact that this is their inherent right under those laws. To address these concerns, data protection increasingly demands dynamic consent procedures, which are challenging to implement with predominantly paper-based permission models.

With the advent of FATCA, the Common Reporting Standards, and other international data sharing agreements in recent years, there has been a significant increase in international data sharing regimes between regulatory agencies in a variety of jurisdictions. Individual identity owners' approval is not necessary before their data is shared since many of these sharing agreements are exempt from data subject consent requirements under national data privacy laws. Financial services is one of the industries where identity data routinely crosses borders, and the data shared between regulatory authorities frequently includes identity data gathered through the KYC process.

Solution: Blockchain Based Refugee Identity System

Since blockchain is a secure way of handing ownership to individuals, it is one of the best ways to implement what should be the norm: the refugee status and their information should belong to the refugees. The relying parties should be able to request the information only. Besides, information should also be specific: if a party needs to know whether a refugee is over 18, they should not have access to that individual's blood group.

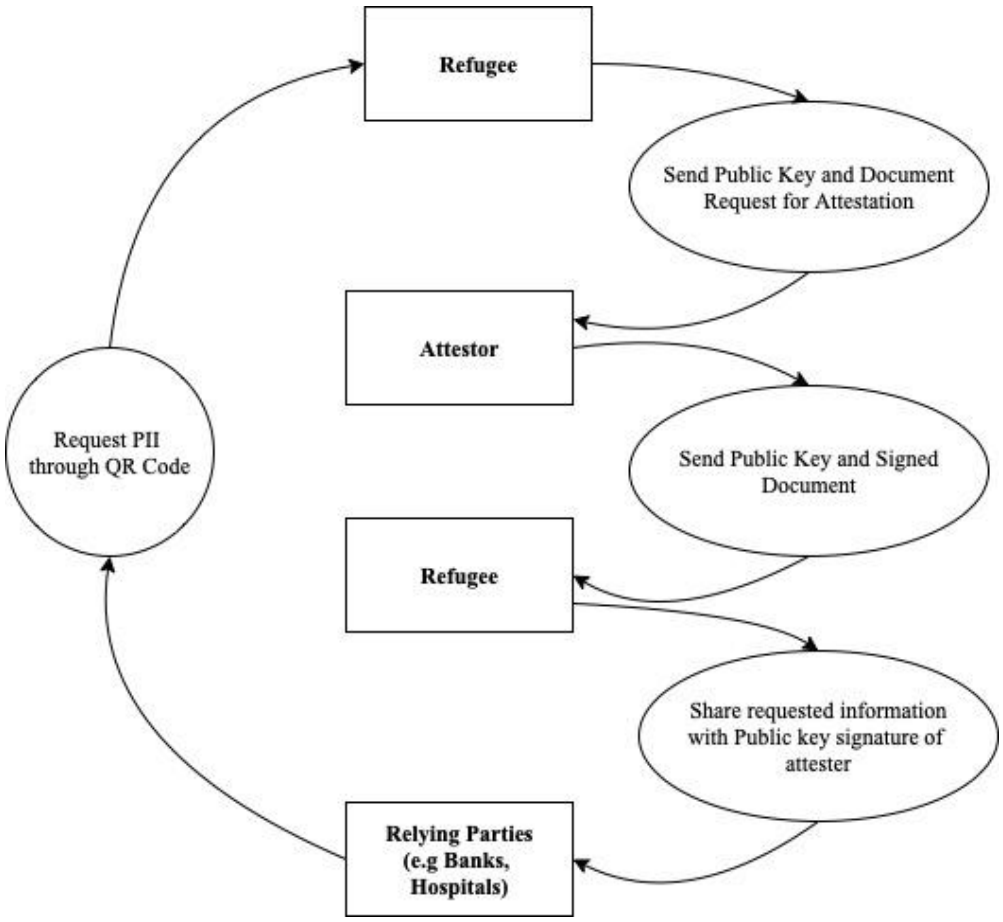
However, that idea itself presents a problem. A refugee cannot just *show* their proof of information to a relying party. It needs to be attested and verified. A naive solution would be to keep every document in the blockchain and keep their attestation mapped, but it would not make the information vulnerable. Therefore, a good solution needs to be –

- Maintains refugee status in blockchain
- Does not store any personal identifiable information (PII) of the refugees
- Keeps a ledger of attestation linked to refugees' documents which is unbacktrackable
- Refugees can request attestations on any PII at their will and send signed information to relying parties
- Refugees manage their own PIIs

How Our Solution Works

Refugee Side

In Astha secure platform, both the registration and verification process is done securely on blockchain. When a potential refugee registers on Astha app, they will get access to a public-private key pair which they can use to conduct further processes. On the in-person screening day, they will get their biometrics and supporting documents taken. After this process is done, the PII (Personal Identifiable Information) will be binded to their unique keys securely in the blockchain. However, the PII will not be stored. By keeping the data in clients' control, Astha makes it harder for hackers to gain sensitive information. Besides, identity fraud and readmission is nearly impossible as the hash of the PIIs is binded to their unique keys in the blockchain.



After screening, the PII provided by the clients will go through a thorough verification in the Astha governance system. After every PII has been verified and accepted, the refugee status on a client will be accepted in the blockchain and the attestations to the PII is written by Astha in the blockchain. Once the procedure is completed, the unique key of the user will be able to provide all verifications needed for entering into the country and enjoying rights. Whenever partners in the Astha governance system need to verify any information, they can request a user's information (e.g Criminal records, Refugee status, Age etc.) through custom QR codes to be scanned by the Astha app. Upon scanning the code, the user can review what information is being requested and decide on exactly what information to send. The information will be automatically attested by Astha and both the information and its authenticity will be sent to the requesting parties. For instance, if a company wants to know if an individual is a refugee and over 18, they can send Astha their driver's license and request for an attestation. Upon request, Astha will send them a public key of their refugee status and another public key of attestation by retrieving the key from a reproducible hash of their driver's license. The individual can then share the public keys with the company and enjoy the products and benefits. This way, the users can control exactly what information they share with the relying parties.

Verifier side

There are a number of different organizations and companies in every governance who issue verifications of authenticity on behalf of identity owners to be used in relying parties. In Astha, the verifiers serve the purpose of verifying client's PIIs after their screening is done.

The attestation needs to be done in a way so that the PIIs are not stored by the validators. To achieve this, Astha organizes the PIIs into Merkle Tree[14], with each node representing a hash of a piece of information and hashes of neighboring nodes. The root hash of the tree can, therefore, represent the PII without storing any parts of it. Fortunately, the only way to get this tree is by rehashing the original document, so clients can prove the existence of identity by supplying the document[15].

Verifiers can be in complete control of their attestation. If, for any reason, they need to revoke the attestation or refugee status, they can do so easily and this will be reflected on the blockchain transaction, ensuring a transparent workflow.

Architecture and Governance

Local Storage vs Decentralized Data Storage
Due to the robust security features of blockchain[16], it might feel natural to store PIIs in the blockchain. However, it only increases the risk of getting those data stolen as while decentralized storage is difficult to manipulate, putting the same data in all nodes means a hacker only needs to hack into one of the nodes to get access to PIIs[17]. As Astha believes the owner of PIIs is only the individual itself, it believes in an individual's rights to store their personal data however they like, and therefore does not store their PIIs, but rather a hash of them.

Biometric Based Key Recovery
Since every element of the refugee ecosystem is accessible using the public-private key pair provided at the beginning, if the key is lost then the refugee will no longer be able to prove their identity. Therefore, it is crucial that no one loses their keys. However, given the situation at most refugee camps, it is very unlikely that every refugee remembers their keys[18]. Therefore, a key recovery mechanism is of utmost importance. As Astha believes individuals should be in charge of their own belongings, it believes that they should be their own "keys". Therefore, the unique key is made from each individual's biometrics[19] (e.g face, iris, fingerprint etc.), so that on the off chance anyone loses their keys, all it will take to recover it will be as simple as presenting themselves.

Foundation
The elected government and its members will be the core foundation of the Astha network. However, they will not be in charge of the total control of the network, but rather enforcing the core principles (e.g granting or revoking refugement for legal reasons) of the network.

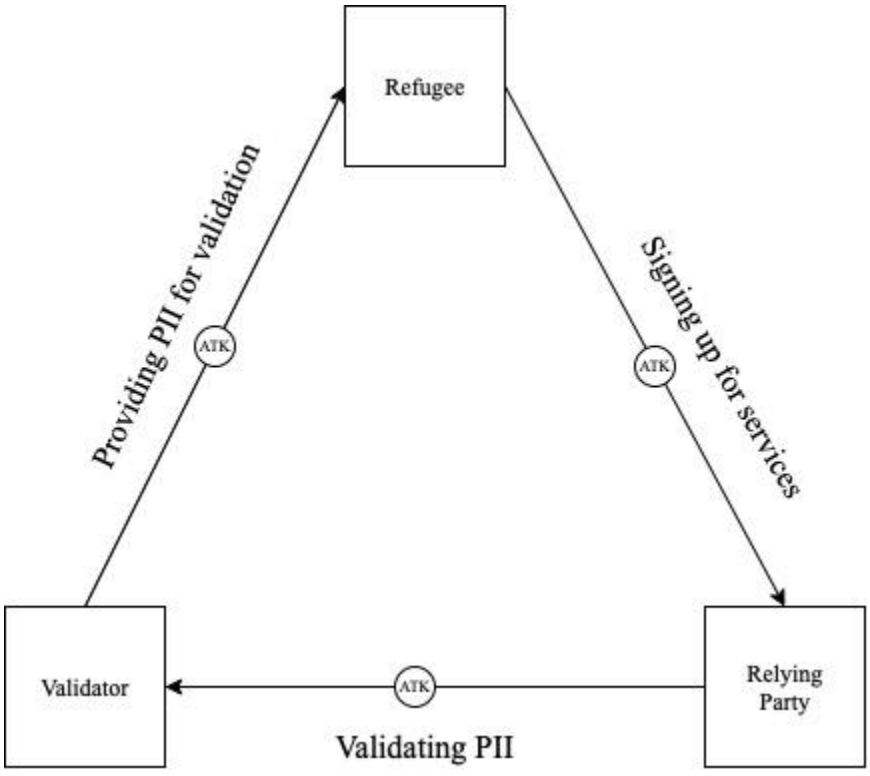
Foundation Core Principles
The Astha Ecosystem is built to solve the problems previously described. In order to do so, it relies on the following core principles –

Transparency
Every transaction, algorithm, framework provided by Astha will be publicly available so that every one in the ecosystem can join to create a trustable network. It will be done by using blockchain[20] and open sourcing all the algorithms.
Data Ownership
Except the refugee status and attestations, Astha will not own any data on any parties in the ecosystem. The clients will be in charge of their PIIs so they can change it, hide it, publicize it at their own will.

Accessibility
Users will be able to access the PIIs whenever they wish. Astha will only be able to prove their existence.

Consent
In order to transfer, modify or hide any of the PIIs, the individual must consent to the action.

<u>The Astha Token (ATK)</u>



For the Astha ecosystem to work smoothly within its components, the Astha Token (ATK) is introduced, a fixed supply of which will be created at the launch of the Astha ecosystem. The Astha ecosystem is mainly made up of three key members : refugees, governance bodies (e.g validators), and relying parties (e.g banks, marketplace). By using ATK as payment mechanism, all products and services will be made available in the Astha ecosystem. The ATK will be paid by the relying parties for completing a transaction which will then be divided into the user and the validators. The proportion, moreover, is easily changeable through the use of smart contracts. This way, the Astha ecosystem incentivizes[21] contributing to the system for all members.

Besides, ATK is used for sharing values in the system. Users can get services such as purchasing from a marketplace, getting bus tickets, opening a fund etc. by trading ATK with relying parties. Astha believes as more parties enter the ecosystem, third parties will offer products and services in exchange for ATK subsequently. ATK can be used in many other services, including but not limited to :

- Bank Account Applications
- Insurance Applications
- Job Applications
- Citizenship through Investment Programs
- Marketplace Listing
- Accessing Medical Facilities
- Coin Exchanges and Trading
- Token Sales
- Precious Metal Purchases
- Business Investments
- Money Transfer Services
- P2P Identity Services

Why ATK Over Regular Tokens

The biggest and most obvious reason for using a dedicated token like ATK for Astha Ecosystem over other established token is controllability in a governance. However, there are other benefits of using ATK over regular tokens, including –

- ATK provides a single and uniform method of settlement across the whole ecosystem.
- ATK incentivizes the essential services in the ecosystem, ultimately increasing its value[22].
- Having a specialized, unique token for the ecosystem provides stability, preventing it from outside effects and volatility.
- Since ATK is a blockchain based ledger system, it utilizes smart contracts to make transactions seamless[23].

Conclusion

Astha proposes a reliable and sustainable method to implement something that should be the norm: refugees' right to own their identity. While one problem can have multiple solutions, this paper shows that this problem can be suitably solved using a fully decentralized blockchain. Refugees need to be protected, and the first step to do so is to protect their identity.

References

1. "WHAT IS WEB 1.0?" TECHNOPEDIA. ACCESSED AUGUST 3, 2017, https://www.technopedia.com/definition/27960/web-10.
2. "INSTEAD OF MERELY READING A WEB 2.0 SITE, A USER IS INVITED TO CONTRIBUTE TO THE SITE'S CONTENT BY COMMENTING ON PUBLISHED ARTICLES OR CREATING A USER ACCOUNT OR PROFILE ON THE SITE…THE UNIQUE ASPECT OF THIS MIGRATION… IS THAT CUSTOMERS ARE BUILDING… BUSINESS(ES) FOR [CORPORATIONS]," QUOTATION FROM ARTICLE ENTITLED "WEB 2.0," WIKIPEDIA, ACCESSED AUGUST 3, 2017, https://en.wikipedia.org/wiki/web_2.0. Accessed 7 May 2022.
3. ROB MARVIN, "BLOCKCHAIN: THE INVISIBLE TECHNOLOGY THAT'S CHANGING THE WORLD," PCMAG, PUBLISHED AUGUST 2, 2017,https://www.pcmag.com/article/351486/blockchain-the-invisible-technologythats-changing-the-world. Accessed 7 May 2022

   SEE ALSO:

   ADAM TINWORTH, "NEXT16: BLOCKCHAIN WILL BUILD WEB 3.0, SAYS JAMIE BURKE," NEXT CONFERENCE, PUBLISHED SEPTEMBER 23, 2016, https://nextconf.eu/2016/09/next16-blockchain-willbuild-web-3-0-says-jamie-burke/. Accessed 7 May 2022

   SIRIKIAT BUNWORASET, "WEB 3.0: ETHEREUM WILL CHANGE EVERYTHING," BANGKOK POST, PUBLISHED JUNE 20, 2017, http://www.bangkokpost.com/business/news/1272219/web-3-0-ethereum-will-changeeverything. Accessed 7 May 2022

   LOS SILVA, "WEB 3.0: HOW DECENTRALIZED APPLICATIONS ARE CHANGING ONLINE CENSORSHIP," ETHNEWS, PUBLISHED FEBRUARY 5, 2017, https://www.ethnews.com/web-30-how-decentralizedapplications-are-changing-online-censorship. Accessed 7 May 2022

   TRISTAN WINTERS, "WEB 3.0 – A CHAT WITH ETHEREUM'S GAVIN WOOD," BITCOIN MAGAZINE, PUBLISHED APRIL 25, 2014, https://bitcoinmagazine.com/articles/web-3-0-chat-ethereums-gavin-wood1398455401/. Accessed 7 May 2022

   "THE BLOCKCHAIN THE NEW WEB 3.0," ACCESSED AUGUST 3, 2017, https://www.moneyoip.com/newweb-3-0. Accessed 7 May 2022
4. "THE RIGHT TO AN IDENTITY – THE GLOBAL SITUATION," HUMANIUM, ACCESSED AUGUST 3, 2017, http://www.humanium.org/en/world/right-to-identity/. Accessed 7 May 2022

5. JEAN CAMP, “IDENTITY IN DIGITAL GOVERNMENT: A REPORT OF THE 2003 CIVIC SCENARIO WORKSHOP,” (AN EVENT OF THE KENNEDY SCHOOL OF GOVERNMENT, HARVARD UNIVERSITY, CAMBRIDGE, MA, 02138, APRIL 28, 2002) http://www.ljean.com/files/identity.pdf. Accessed 7 May 2022
6. BEN SCHILLER, “2 BILLION PEOPLE ARE STILL LEFT OUT OF THE MODERN FINANCIAL SYSTEM: HOW QUICKLY CAN WE CHANGE THAT?,” FAST COMPANY, PUBLISHED NOVEMBER 3, 2015, https://www.fastcompany.com/3051846/2-billion-people-are-still-left-out-of-the-modern-financial-systemhow-quickly-can-we-change. Accessed 7 May 2022
7. RAVI RAJA KONATHALA, “WHAT ARE THE PRIVACY ISSUES WITH AADHAAR?”, QUORA (QUESTION-AND ANSWER FORUM), APRIL 5, 2017, https://www.quora.com/what-are-the-privacy-issues-with-aadhaar. Accessed 7 May 2022
8. TECH2 NEWS STAFF, “MASSIVE SWEDISH DATA BREACH REVEALS SWEDISH MILITARY SECRETS AND THE IDENTITY OF ALMOST ALL ITS CITIZENS,” TECH2, PUBLISHED JULY 26, 2017, http://www.firstpost.com/tech/news-analysis/massive-swedish-data-breach-leaks-swedish-military-secretsand-the-identity-of-almost-all-its-citizens-3855113.html Accessed 7 May 2022
9. “A BLUEPRINT FOR DIGITAL IDENTITY: THE ROLE OF FINANCIAL INSTITUTIONS IN BUILDING DIGITAL IDENTITY,” WORLD ECONOMIC FORUM, PUBLISHED IN AUGUST 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf. Accessed 7 May 2022
10. “DATA BREACH TRACKER: ALL THE MAJOR COMPANIES THAT HAVE BEEN HACKED,” TIME, PUBLISHED OCTOBER 30, 2014, http://time.com/money/3528487/data-breach-identity-theft-jp-morgankmart-staples/ Accessed 7 May 2022
11. AMBROSE MCNEVIN, “THE FIVE BIGGEST ISSUES IN IDENTITY MANAGEMENT AND WHAT’S BEHIND THEM," COMPUTERS BUSINESS REVIEW, PUBLISHED MAY 20, 2016, http://www.cbronline.com/news/cloud/the-top-five-issues-in-identity-management-4899761/. Accessed 7 May 2022
12. SEE SUBHEADING “KYC-CHAIN” UNDER HEADING “USE CASES:”, UN-BLOCKCHAIN, https://unblockchain.org/use-cases/identity-under-construction/. Accessed 7 May 2022
13. WIKIPEDIA CONTRIBUTORS, "SEMANTIC WEB," WIKIPEDIA, THE FREE ENCYCLOPEDIA, ACCESSED AUGUST 3, 2017, HTTPS://EN.WIKIPEDIA.ORG/W/INDEX.PHP?TITLE=SEMANTIC_WEB&OLDID=793179594. Accessed 7 May 2022
14. “Merkle tree.” *Wikipedia*, https://en.wikipedia.org/wiki/Merkle_tree. Accessed 5 May 2022.
15. “Using MerkleTree for Blockchainized Document Certification.” *Laurent Senta*, 13 September 2021, https://laurentsenta.com/articles/blockchain-merkle-tree-algorithm/. Accessed 5 May 2022.

16. “What is Blockchain Security?” *IBM*, https://www.ibm.com/topics/blockchain-security. Accessed 5 May 2022.
17. Magas, Julia. “Blockchain Storage Offers Security, but Leaves Data Transparent.” *Cointelegraph*, 1 March 2020, https://cointelegraph.com/news/blockchain-storage-offers-security-but-leaves-data-transparent. Accessed 5 May 2022.
18. Goldhill, Olivia. “Photos: What Syrian refugees carry in their bags as they leave their lives behind.” *Quartz*, 6 September 2015, https://qz.com/496220/photos-what-syrian-refugees-carry-in-their-bags-as-they-leave-their-lives-behind/. Accessed 5 May 2022.
19. Salman, Duha & Azeez, Raghad & Hossen, Adul. (2020). Key Generation from Multibiometric System Using Meerkat Algorithm. Engineering and Technology Journal. 38. 115-127. 10.30684/etj.v38i3B.652.

20. “How Does Blockchain Technology Ensure Transparency In Cryptocurrency Trade?” *NDTV.com*, 18 November 2021, https://www.ndtv.com/business/how-does-blockchain-technology-ensure-transparency-in-cryptocurrency-trade-find-out-2614495. Accessed 5 May 2022.
21. “Tokens can better incentivize startup employees than equity.” *TechCrunch*, 9 September 2018, https://techcrunch.com/2018/09/09/tokens-can-better-incentivize-startup-employees-than-equity/. Accessed 5 May 2022.
22. Gogol, Frank. “How cryptocurrency gains value -- Everything you need to know [2022].” *Stilt*, 26 April 2022, https://www.stilt.com/blog/2021/07/how-does-cryptocurrency-gain-value/. Accessed 5 May 2022.
23. “Blockchain Smart Contracts: Changing the Way Business is Done Today.” *AlvaradoSmith*, 1 April 2021, https://www.alvaradosmith.com/your-vendor-wants-you-to-use-a-blockchain-smart-contract-for-the-transaction-now-what/. Accessed 5 May 2022.