# Appendix-Solution Design

*The Hyperledger Aries/Indy blockchain framework*

The solution that emerged from the methodological steps described above builds upon Hyperledger Aries/Indy (HAI), which is an open source blockchain framework maintained by the Linux Foundation that proposes a new trust layer for the internet (see Figure A.1). It is a blockchain framework specifically oriented towards a decentralized identity management use case and thus well-aligned with the motivating philosophical and design ideas that underpin this project. HAI is comprised of four basic components: 1) verifiable claims, 2) peer-to-peer agents, 3) decentralized identifiers, and 4) a distributed ledger. Verifiable claims are a “machine-readable statement made by an entity that is cryptographically authentic (non-repudiable)” (W3C, 2019).



Figure A.1: Overview of Hyperledger Airies/Indy Trust Stack (Source: adapted from Bouma, 2019).

Verifiable claims are made when a “holder” agent sends a cryptographic credential – provable digitally signed data - received from an “issuer” agent to another “verifier” agent across a peer-to-peer connection which the receiving verifier agent is able to cryptographically prove is authentic (see Figure A.2). Each interacting agent has a decentralized identifier - a new type of identifier for verifiable, “self-sovereign” digital identity that is independent from any centralized registry, identity provider, or certificate authority (W3C, 2019; DIF, 2019) - used to facilitate communication in each pairwise connection. HAI employs privacy-enhancing techniques, such as selective disclosure and zero-knowledge proofs – a cryptographic technique allowing an agent to prove that they know something, such as a password, without revealing what they know. A distributed ledger – a ledger that is shared across a set of nodes (i.e., network endpoints) and synchronized between the nodes using a consensus mechanism (e.g., Redundant Byzantine Fault Tolerance) – is used to store Public DIDs (e.g., of issuer agents), data schemas for credentials, credential definitions, and revocation registries – that enable the cryptographic verification of claims.



Figure A.2: Hyperledger Aries/Indy Overview (Source: Anon Solutions).

*The Health Data Sharing Platform*

The Health Data Sharing platform has four main actors: 1) MYco, which is an issuer of individuals’ health credentials; 2) Ethics Review Boards (ERB), which issue ethics credentials to researchers so that individuals can verify that their data will be handled properly when shared; 3) Researchers, who apply to the ERB to conduct research projects and market these to data owners; and 4) Data Owners, MYco clients who hold health credentials issued by MYco that are shared with researchers with the data owner’s consent.

The platform is designed to support a number of processes relating to the sharing of data needed to conduct personalized health research. Figure A.3 represents a high-level overview of the solution’s business flow.



Figure A.3: Overview of private and secure health data sharing process.

The first step in the process of data owners sharing their data and receiving rewards for their contributions occurs when they request cryptographic credentials for each of their biomarkers. MYco then issues these credentials to the personal health wallet of each individual data owner (MYco client).

The solution also supports researchers’ application to an ERB for ethics certificates to conduct their research, and once approved, the sending of the ethics certificate in the form of a cryptographic credential to the wallet of the applicant/researcher. Once they have ethics approval, researchers are then able to use the platform to advertise their research projects to data owners.

When a data owner notices a research project in which s/he would like to participate, this initiates a “handshake” process using a HAI blockchain network in which data owners verify that the research project has the necessary ethics approval and researchers verify that data owners meet their study criteria and consent to the sharing of their data. The process completes when data owners share the specific health data (e.g., biomarkers) needed for the study and researchers send data owners a reward for their participation in the study in the form of a cryptographic credential. The reward adheres to principle six of GA4GH and is meant to recognize data owners for sharing their data in a manner that is meaningful and appropriate.

Figure A.4 represents a visual overview of the handshake process that takes place between data owners and researchers on the platform. A key feature of the entire handshake process is its alignment with the motivating theoretical and design principles; that is, the solution is designed to ensure that the identity of data owners is never revealed to researchers, no personal health information is ever recorded or stored on the blockchain, and data owners remain in control of their personal health information at all times, revealing only as much information as they feel comfortable with given their assessment of the risk-benefits of the transaction.



Figure A.4: Wireframe showing Handshake Process.

**REFERENCES**

W3C Community Group. (2019). *Decentralized Identifiers (DIDs) v0.11: Data Model and Syntaxes for Decentralized Identifiers (DIDs)*. Retrieved from <https://w3c-ccg.github.io/did-spec/> (accessed January 23, 2021).

(DIF) Decentralized Identity Foundation. (2019). *Together We’re Building a New Identity Ecosystem*. Retrieved from [https://identity.foundation/](https://identity.foundation/.) (accessed January 23, 2021).