PhiDDLeR/FiDDLeR

Personhood Identification Data Layer & Encryption Resource protocol (Federated)

Identification and sovereignty over identifying information are issues that plague us more today than they did when the concept of ID were first introduced by King Henry V of England in 1414, and even more than during the First World War when the concept of national passports was globally adopted. It seems like it has always been the responsibility of some government bureaucrats to regulate these ID systems, which of course leads to fraud and corruption. They require increasingly more personal information, under the guise of verification, and in exchange for some benefit (like social security payments or the ability to drive or travel to another country. Granted, over the last few decades, technology has aided the government in doing a more thorough job by making identification documents harder (but still possible) to counterfeit. But still, identity is not something that people can own for themselves, independent of governments. Furthermore, very often, identification documents are not free. Even the liberal state of California, a sanctuary for the homeless, charges the homeless a reduced rate of $6 for an ID card.

This is why we devised a system by which…
Users can create their own identity files for free. The base ID file (person.id) is a json file with general information about the person. Each record in the file can have plain or encrypted data and is accompanied by an ID. Files can be posted to ipfs and must be validated before additional associated files may be posted. Once validated, a non-transferable, no-fungible token FID is issued to the user's wallet. Associated files may be added ad-hoc (education.id, studies.id, employment.id, experience.id, interests.id, pets.id, criminal.id, wallets.id, athletics.id, lineage.id, projects.id, volunteering.id, skills.id, patents.id, travel.id, robot.id, vehicle.id, contacts.id, etc). Such files are in the same format as person.id (and there can also be other species like dog.id, bird.id, etc). Each record may have any number of certification files corresponding to the identifier of the record. Those certifications may be posted by a certified certification authority (CCA), and may contain confirmation of the data, method of confirmation, confidence % of confirmation and so forth. Additionally, each CCA will have a trust score of its own.

Anyone can share their FID with others to prove they are who they say and that they have specific credentials. Those credentials may have varying degrees of certainty or trustworthiness (depending on the verifier or lack thereof), but may also be verifiable to a higher degree (such as a government, school or employer) if the individual or requester is willing to pay for higher forms of verification. Some automated verification methods can be employed (such as Turing tests), and other methods can be manual (such as reverse Turing tests or social verification), and yet others can be biometric in nature. FIDs come with the added benefit that they can be used for federated login via social channels.

Verification (or personhood ID lookup) will cost some amount of $Phidl each time a verification happens, the person can be notified if a request for their ID docs occurs, and depending on some options, they may get reverse lookup info for some amount of $Phidl.

Note that such identification is not limited to humans. Any noun can be assigned and have credentials proven such as companies, buildings, even species. Furthermore, anyone can suggest updates to the credentials of files they do not own via wikipedia style approval system.