Uport: Self-sovereign Identity and Reputation

What is the business case, area, or topic that this use case applies to?

Digital Identity

What problem are they trying to solve?

uPort aims to return ownership of digital identity to the individual. Currently, a digital identity is established when a nation-state, company, or other organization is able to say and prove that an individual exists. There are not broadly legitimate ways for an individual to create a digital identity for themselves without engaging with these intermediaries. The result is that digital identity is fragmented across multiple systems controlled by nation-states, companies, and other organizations.

What is the value created by solving this problem?

An identity is central to almost every transaction that occurs in the physical world and the digital world. In the digital world, most identities are siloed and controlled by centralized entities - like your email, your banking information, and your healthcare account. By creating a digital identity that is centered around the user of that identity, the user has ultimate control over their identity and is the final arbiter of who can access and use their data or personal information. The value created is for the individual - the individual has control of their identity and the data associated with that identity.

Do they need a database?

Yes. uPort needs a database because they are creating and storing identities

Does it require shared write access?

Yes, anyone should be able to use uPort in order to create an identity.

Are any of the parties unknown or untrusted? Or if they're trusted is it possible for them to have conflicting interest?

Anyone should be able to participate in the system, and it should not be possible to prevent anyone from creating an identity. Therefore, all parties can be assumed to be unknown.

How will a blockchain be applied to this use case?

A blockchain is required to create an identifier (an Ethereum address) and a public-private key pair for signing transactions. The registry of identities on Ethereum allows for information about an identity - whether that be a degree earned or a permission granted to that identity - to be sent to and held by the holder of that identity. This information about an identity is referred to as a claim or attestation, and allows for the holder of the identity to accrue and use information associated with their identity.

Which component pieces will be utilized?

Public key cryptography allows for users of uPort to sign attestations. So a hospital could registry an identity with uPort, and then send attestations to patients who share their uPort identity with the hospital. Signing a message with the information about what happened during a hospital visit would be an example of how a component piece of the blockchain is used.

Will the blockchain used be public, private, or consortium and why?

uPort is built on top of the public Ethereum blockchain. The public chain is used so that any identity can be verified, as that information is available to all participants in the blockchain.

Is a token used (to digitize an asset, store value, or to provide access to the blockchain, for example)? Why is it needed and how will it be used? If a token is not utilized, why is ETH or another native token able to be used?

No token is used other than ETH. ETH is used to pay for any transactions occurring on the public blockchain. As uPort supports off-chain transactions, like attesting to a claim, ETH does not have to be used every time an attestation is issued.

Are there overlay networks that will need to be utilized in order to make this use case operate? If so, what are they? If not, why does the existing infrastructure work?

A user's public key is stored on IPFS, which allows for others to verify any attestation that the user has made about herself or to other users.

Are there other factors to consider in this use case?

Private keys are currently kept on the mobile device on which the uPort identity is created. Therefore, uPort developed a data recovery and backup option utilizing a seed phrase. When an individual sets up their uPort, they write down the seed phrase - which is a series of words. If the user were to lose their mobile device, they could download the uPort app onto a new device, and use the seed phrase during setup to recovery the identity they previously created. This is very important, as establishing a digital identity on a device means that consideration must be given to how to recover information associated with that identity if the device were to be lost or stolen.