Decentralized Identity Management

DID Creation with Ethereum

W3C Decentralized Identifiers (DIDs) are usually the identifier of choice used for SSI ecosystems.

1. What is the main advantage of DIDs compared to blockchain accounts?

   The main advantage of DIDs compared to blockchain-like accounts is the flexibility provided by the DID document. Because of it, keys can be updated, and additional meta information can be given in a standardized way.

2. Briefly explain what a DID resolver is and what it returns.

   A DID resolver is a piece of software resolving a DID into a DID document by following a pre-defined algorithm specific to the DID's method. It returns a DID document is a document that is accessible to anyone by resolving a DID and contains information related to a specific decentralized identifier, such as the currently used public key and usage conditions.

3. How are DID method standards governed?

   They are not. Anyone can create a standard and distribute it.

4. What are the minimum steps to create a did:ethr? Read the document at: https://github.com/uport- project/ethr-did

   (a) Generate a new Ethereum account
   (b) Concatenate "did:ethr" + address

Using DIDs and Verifiable Credentials in Healthcare

Bob, a patient, uses a Decentralized Identifier and Verifiable Credentials to streamline the process of sharing his medical records with healthcare providers.

1. Bob wants to use his SSN as his subject identifier in VCs issued for him. Can he do it, and should he do it? Why or why not?

   Yes, he can do it because DIDs are not technically the only possible identifiers usable with VCs. However, he should probably not do it because then he would not have a private key to prove his identity in VPs.

2. What 3 parts does a Verifiable Credential consist of?

   Credential Metadata, Claim(s), Proof(s)

3. Name the three main roles involved in the lifecycle of a verifiable credential and name the corresponding actors in this specific example.

   Holder (or Subject) is Bob, Issuer is a healthcare provider, Relying Party is a healthcare provider

4. Is this a good use case scenario for VC and DID? Explain your reasoning, highlighting any benefits and drawbacks of using these technologies in this context.

It probably is a good use case scenario.
Advantages: Privacy, security, efficiency
Disadvantages: Technical knowledge, potential for Bob to lose his data, possibility of someone leaking verifiable health data to criminals

5. SSI is often advertised as "gaining sovereignty about your own data". Does Bob gain that? Argue.

Bob does not necessarily gain full control over his data. If he hands over data to a healthcare provider, that provider probably must store it for some time and could (intentionally or not) forward that data. Bob gains the sovereignty of interacting with services on his own behalf, but he has no direct control over his data once it was handed over. There are legal boundaries like GDPR, but they can be broken.

6. SSI is still not widely used. Usability for end users is an issue. Name and briefly explain two concrete problems that wallets have to overcome.

key and credential recovery, support of different DID methods, support of more than one interaction protocol to achieve a "universal" wallet