

Identity and SSO on Blockchain



What is Personal Identity ?

Anything that can uniquely identify and verify an individual

1. Government/Institutional Identity

Example : SSN, Passport

Problems :

- Identity Theft
- Lack of real-time verification



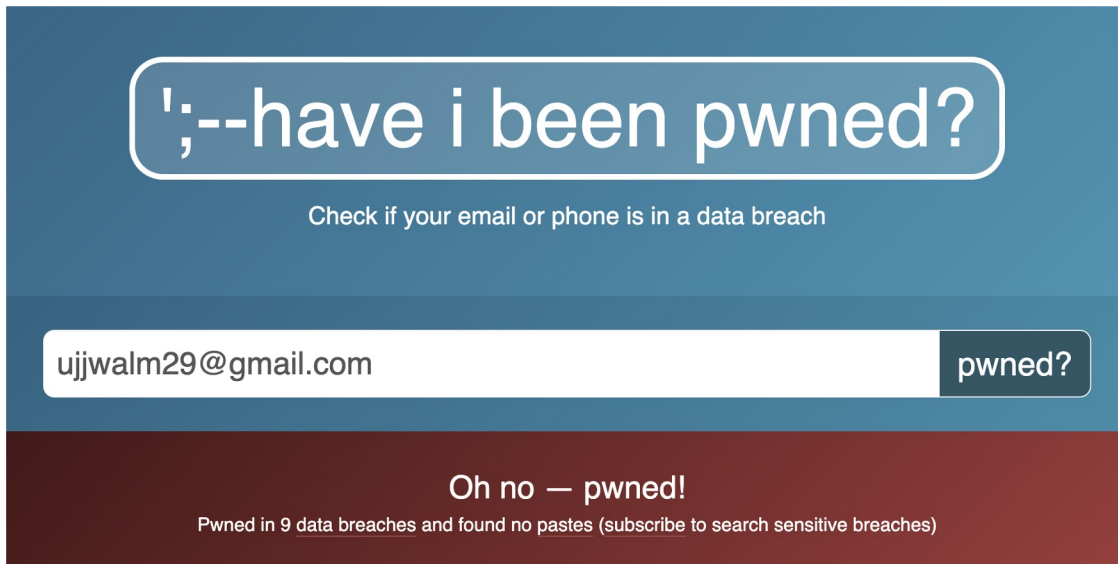
What is Personal Identity ?

2. Digital Identity

Example : Google OAuth

Problems :

- Data Leaks
- No Control



';--have i been pwned?

Check if your email or phone is in a data breach

ujjwalm29@gmail.com pwned?

Oh no — pwned!

Pwned in 9 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

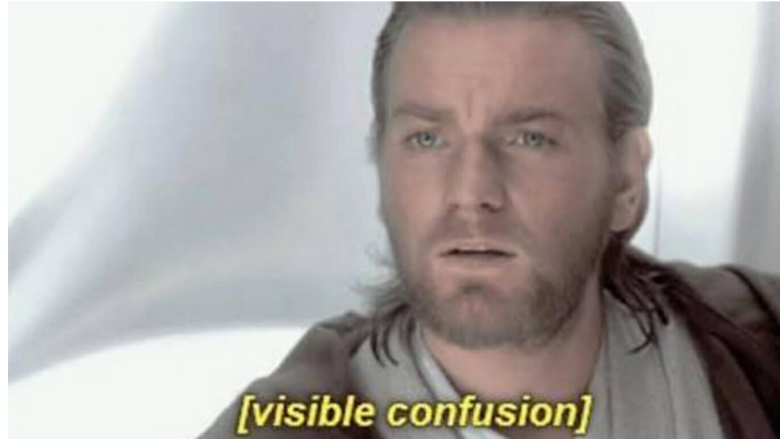
Identity On Blockchain ?

A Public blockchain is

- Trustless
- Permissionless
- No privacy

Personal Identity

- Trusting an authority
- Only trusted people should use
- Private

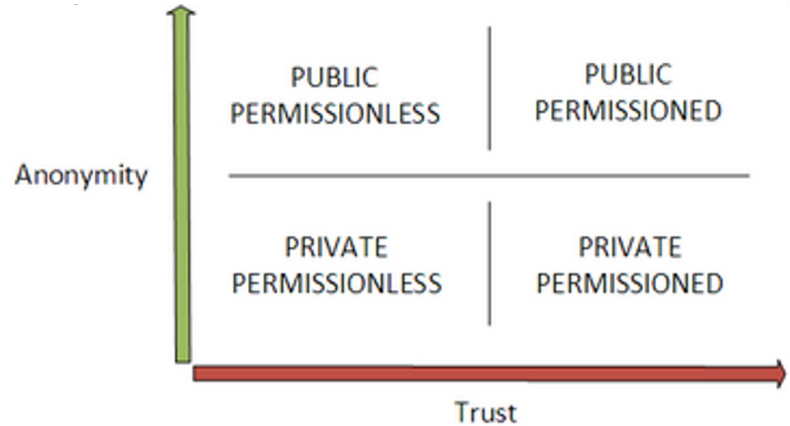


How do we design public and permissioned IAM systems?

To maintain high trust and anonymity.

Let's go through a few key terms and con

- DID
- Verifiable Claims
- Revocation
- Identity management



DID

- Stands for Decentralized Identifier
- A unique anonymous identifier for an entity on the blockchain.
- It can refer a user, organization, document, data model.
- Every DID refers to a unique DID document stored in a decentralized DB.



Scheme

did:example:123456789abcdefghijklmnopqrstuvwxyz

DID Method DID Method Specific String

DID Document

- A JSON-LD object that is stored in a decentralized database or file system.
- Persistent and Immutable.

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    // this key can be used to authenticate as DID ...9938
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }]
}
```

Verifiable Claims

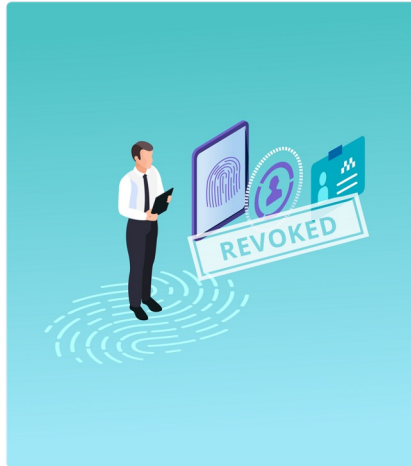
- A document that reveals some information about an entity whose authenticity can be verified.
- It is trustworthy and tamper proof because it is signed by the claim's issuer.
- Claims can reveal only a subset of information about an entity. a

```
{
  "@context": "https://w3id.org/security/v1",
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2010-01-01",
  "claim": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "revocation": {
    "id": "http://example.gov/revocations/738",
    "type": "SimpleRevocationList2017"
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavE1l0/I1zpYw8XN1lbgVg/sCne04Jugez8Rw0g/+MCRVpj0boDoe4SxxKjkC0vKiCHGdvc4krqi6Z1n0UfqzxGfmatCuFibcC1wpsPRdW+gGsutPTLzvueMwmFhwYmfIFpbBu95t501+rSLHIEuuJM/+PXr9Cky6Ed+W3JT24="
  }
}
```



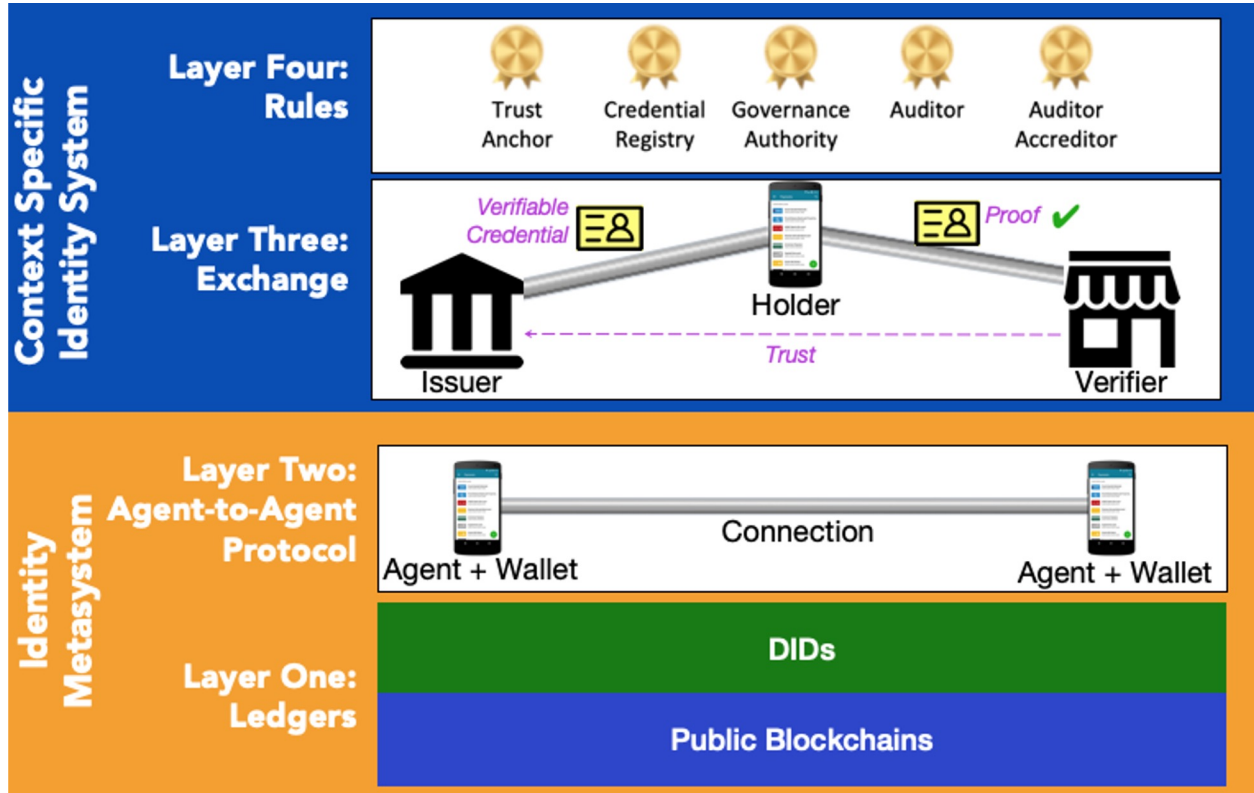
Revocation of Claims

- The issuers have the ability to revoke a verifiable claim using revocation lists.
- Revocation lists can be maintained in the same blockchain or in a separate blockchain.
- The verifiers will use these revocation lists to check the validity of the corresponding claims.



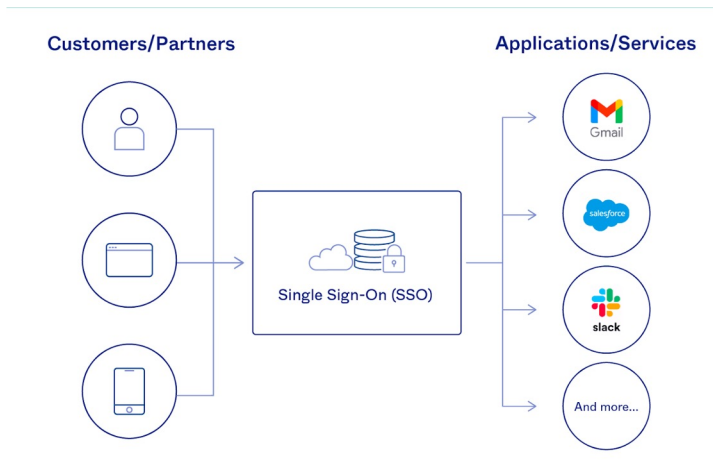
Existing System Review: Sovrin

- Based on Sovrin's protocol operating on the Sovrin ledger.



Use case: SSO (Single Sign On) Infrastructure

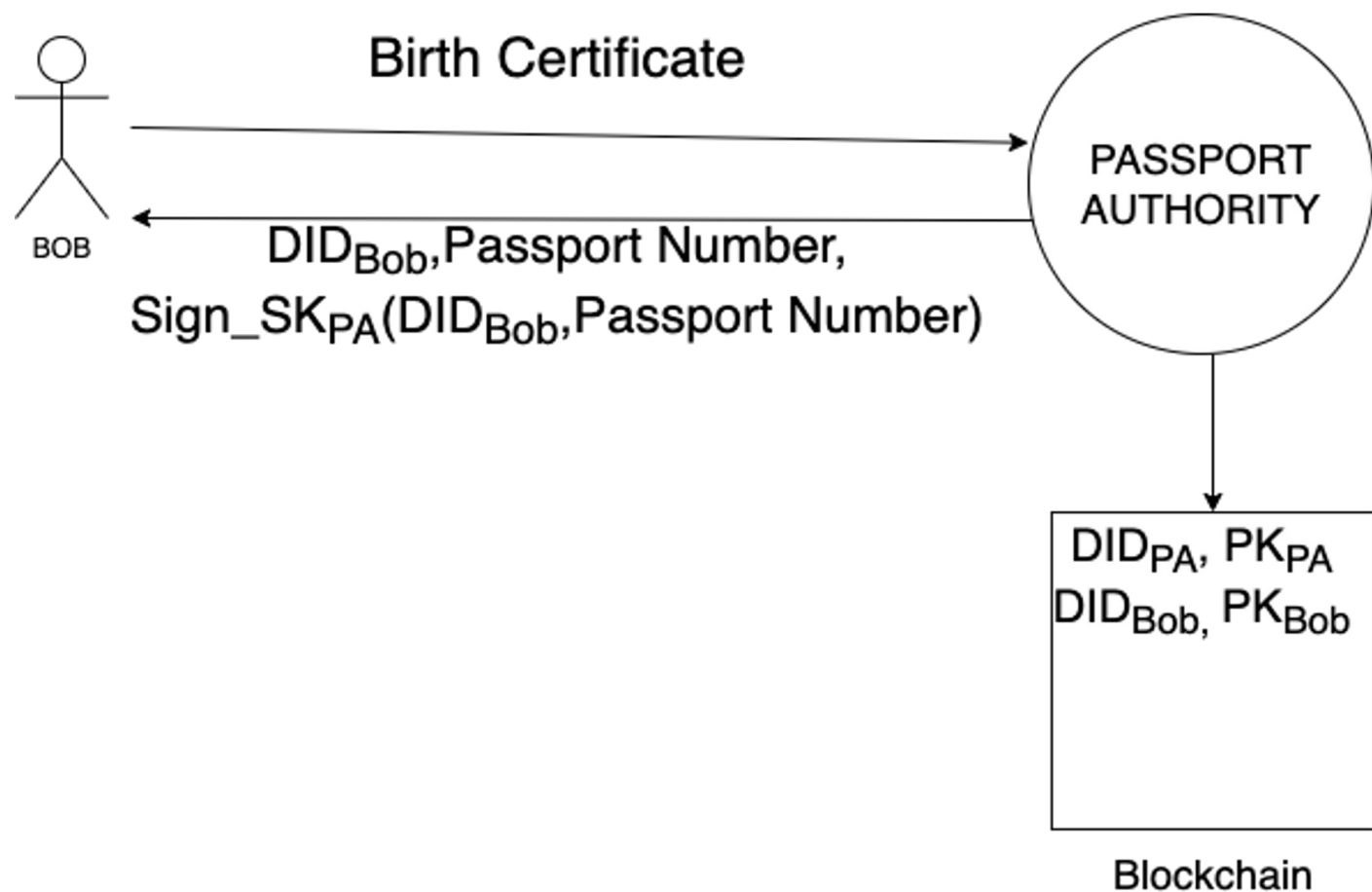
- Allows the user to login once and access services without re-entering authentication factors. (Zoom, Google etc.)
- Involves transfer of data between centralized services. User has no control
- Our solution : SSI in SSO. Give the control of information back to the users.
- Decentralized Public Key Infrastructure (DPKI)



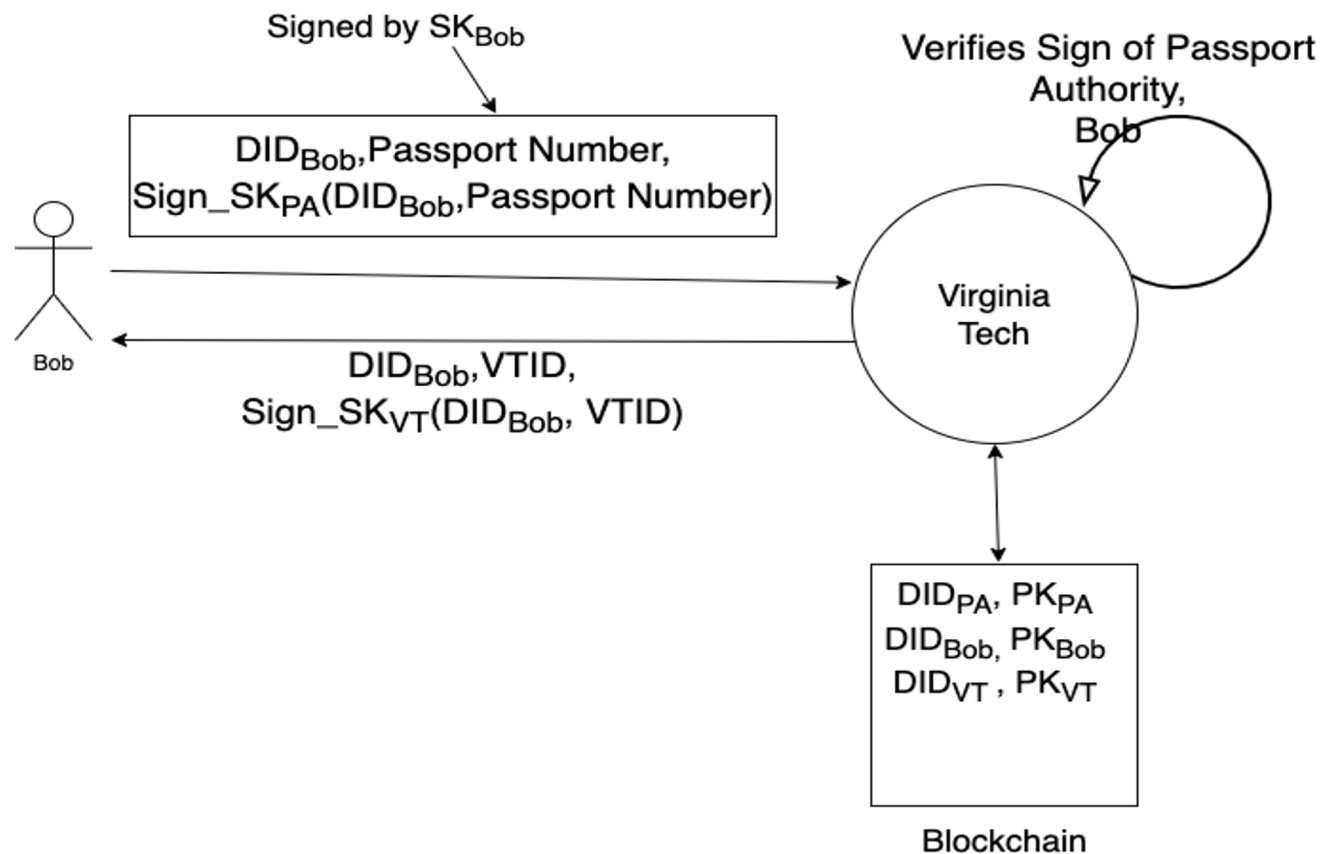
Proposed system design

- **Permissioned blockchain**
 - User
 - Authorities
 - services

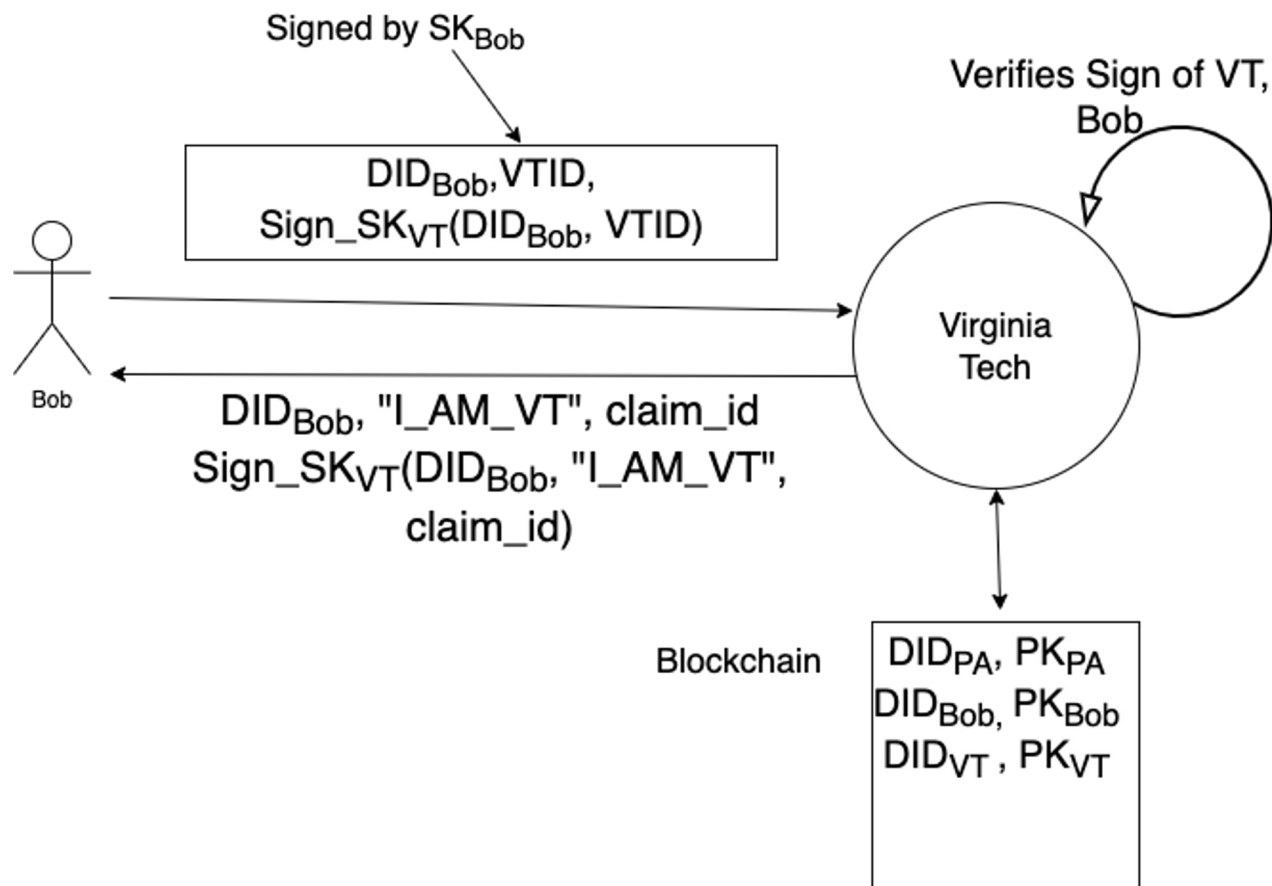
Step 1:



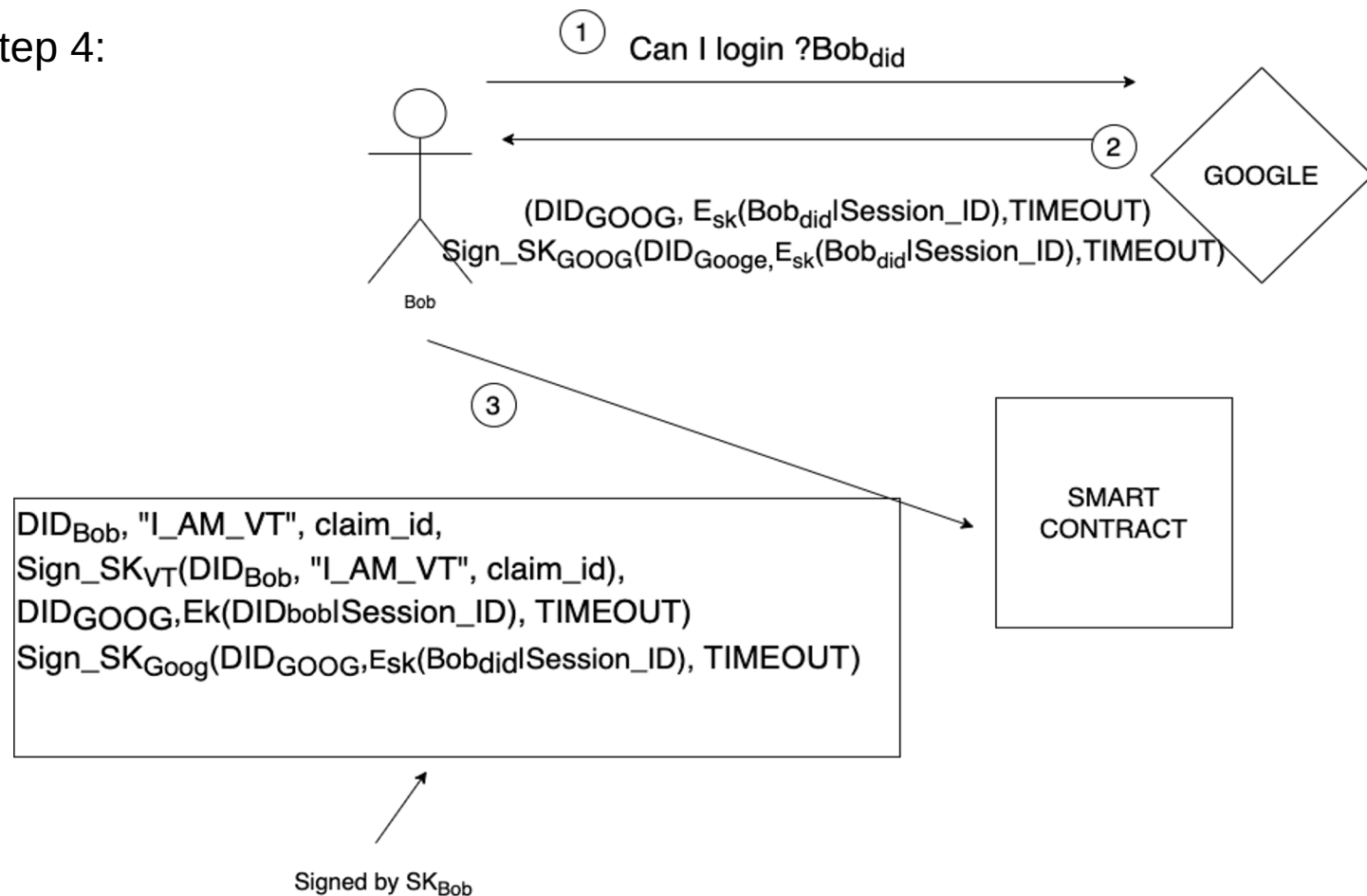
Step 2:



Step 3:

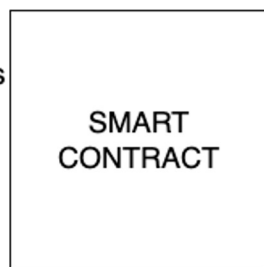


Step 4:



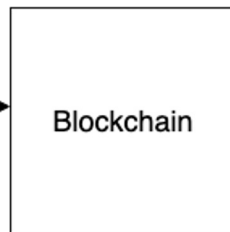
Step 5:

①
Validates Signatures
and the Claim



$DID_{Goog}, E_{sk}(DID_{bob} | Session_id), TIMEOUT$

② Create Transaction

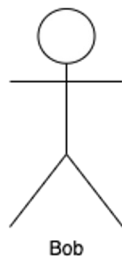


③

New block transmitted

⑤

Access Token



GOOGLE

④

When DID_{Goog} is found
Decrypt the message, find the recipient & session_ID.
Create Access Token with TIMEOUT

Advantages of Identity on Blockchain

Decentralised

No single Authority has control

Availability

System prioritises availability

Self-Sovereign

Control of data to the user

Summary

- Examined concepts of Identity
- Looked at Self Sovereign Identity
- Current existing systems of Identity Management on the Blockchain
- Proposed a new System of Identity management

Thank you!

