SEC-205: Distributed Ledger and Blockchain

Lecture 7: Decentralized Identity

Instructed By:

Dr. Charnon Pattiyanon

Assistant Director of IT and Instructor
CMKL University

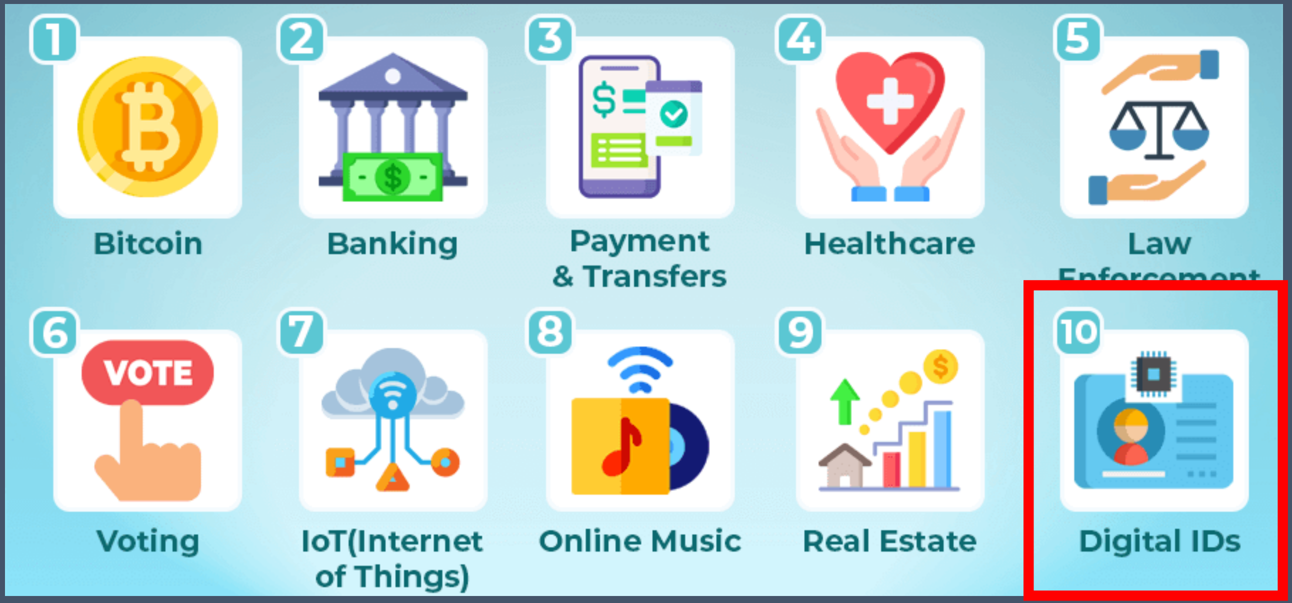
Artificial Intelligence and Computer
Engineering (AICE) Program

Today's Agenda

- In today's lecture, we will explore and learn about:
  - Detailed Background on Identity and Access Management System.
  - The problem with Centralized Identity and its Evolution.
  - Decentralized Identity and Self-Sovereign Identity

Applications of Blockchain Technology

- Since the blockchain technology provides a decentralized and immutable way to store transactional data over the distributed and peer-to-peer network, it can be applied to many domains apart from decentralized financial applications, such as Bitcoin or Cryptocurrencies.

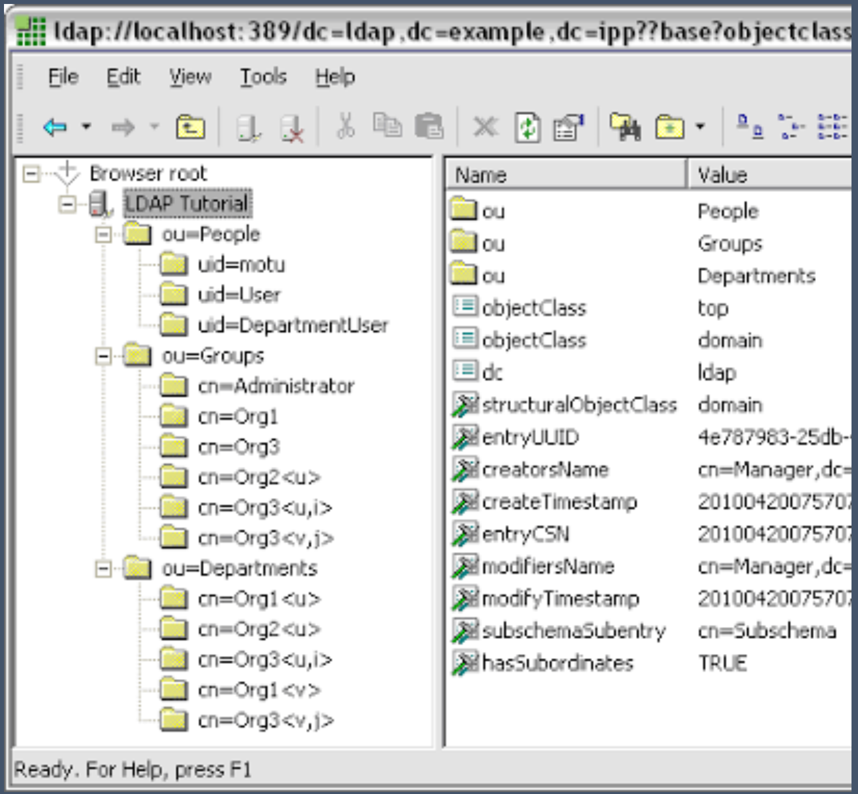


Basic Terminologies of Identity and Access Management

- **Identity (ID):**
  - A digital asset that identifies an individual
  - Incl. human identity, machine, device, or other digitized assets
- **Personal Information (PI):**
  - (GDPR, 2018) Any information relating to an identified or identifiable natural person.
- **Personal Identifiable Information (PII):**
  - (NIST, 2010) Any information about an individual maintained by an agency, including:
    - (1) Any information that can be used to distinguish or trace an individual’s identity.
    - (2) Any other information that is linked or linkable to an individual

Basic Terminologies of Identity and Access Management

- **Lightweight Directory Access Protocol (LDAP):**
  - You can think of *a hierarchical-structured user database.*
  - Its advantages over database is speed of read, but the entry writing performance is obviously worse that database.
  - Some well-known LDAP applications are Active Directory, IBM Tivoli, Oracle Unified Directory



ldap://localhost:389/dc=ldap,dc=example,dc=ipp??base?objectclass

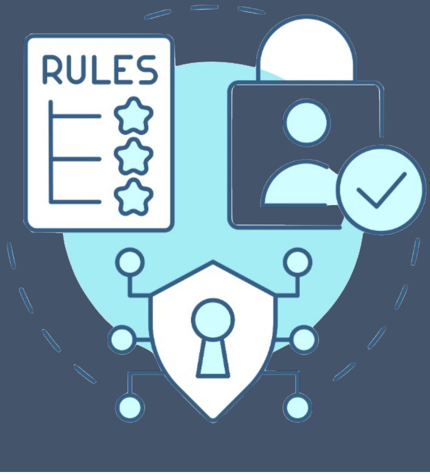
- Browser root
  - LDAP Tutorial
    - ou=People
      - uid=motu
      - uid=User
      - uid=DepartmentUser
    - ou=Groups
      - cn=Administrator
      - cn=Org1
      - cn=Org3
      - cn=Org2<u>
      - cn=Org3<u,i>
      - cn=Org3<v,j>
    - ou=Departments
      - cn=Org1<u>
      - cn=Org2<u>
      - cn=Org3<u,i>
      - cn=Org1<v>
      - cn=Org3<v,j>

Name	Value
ou	People
ou	Groups
ou	Departments
objectClass	top
objectClass	domain
dc	ldap
structuralObjectClass	domain
entryUUID	4e787983-25db-
creatorsName	cn=Manager,dc=
createTimestamp	2010042007570
entryCSN	2010042007570
modifiersName	cn=Manager,dc=
modifyTimestamp	2010042007570
subschemaSubentry	cn=Subschema
hasSubordinates	TRUE

Ready. For Help, press F1

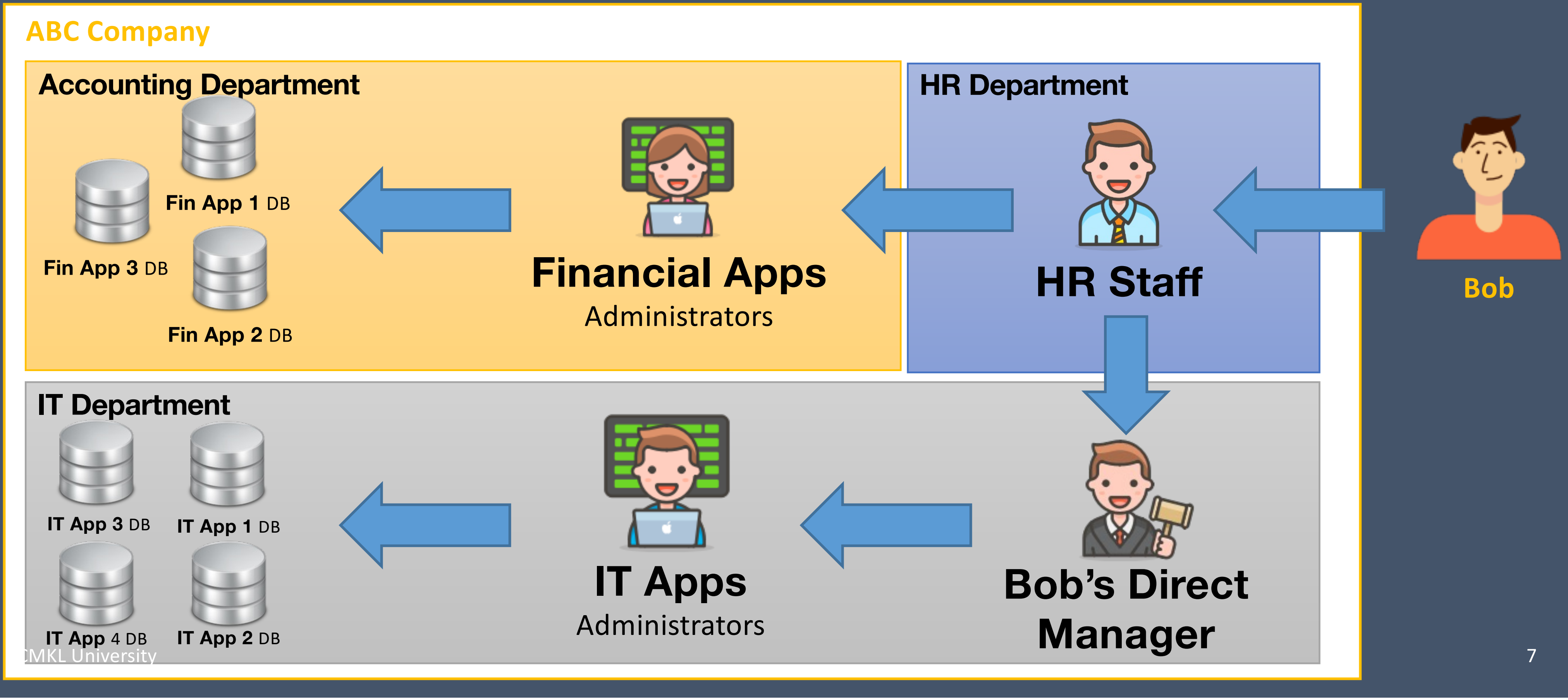
Basic Terminologies of Identity and Access Management

- **Identity Management:**
  - (Microsoft) Identity management checks a login attempt against an identity management database, which is an ongoing record of everyone who should have access.
- **Access Management:**
  - (Microsoft) Access management keeps track of which resources the person or thing has permission to access.
- Most of the time, both are combined and called as **Identity and Access Management (IAM)**.



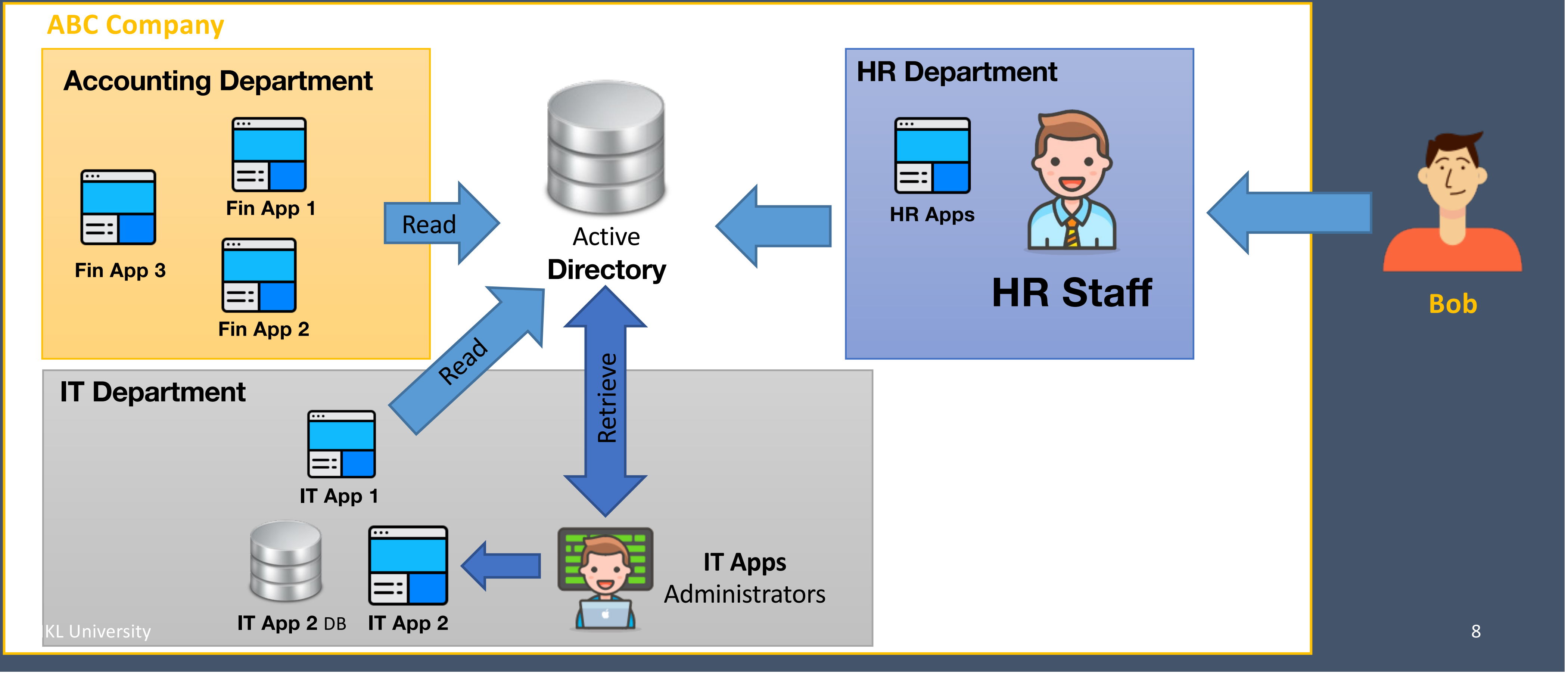
Identity and Access Management Systems

- **Phase 1: Centralized Identity**



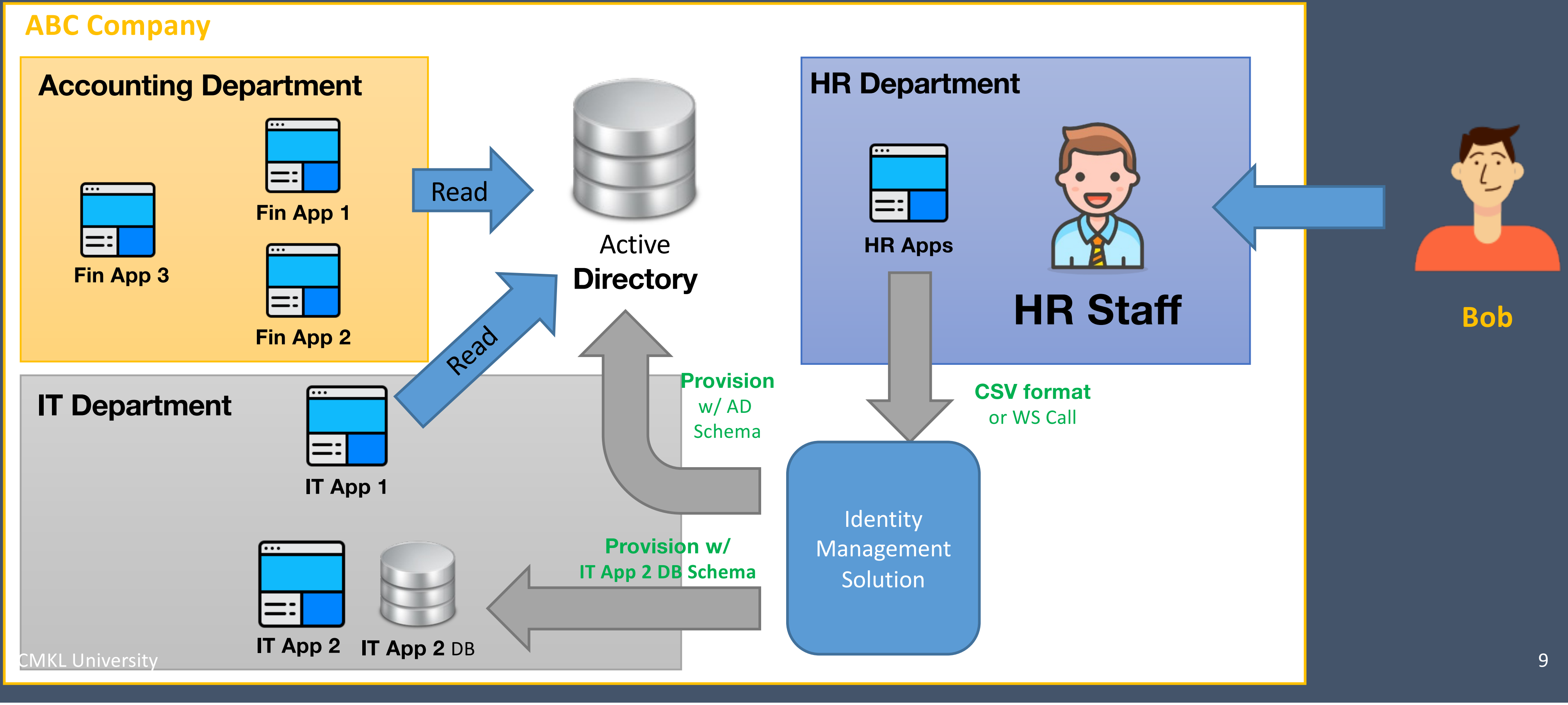
Identity and Access Management Systems

- **Phase 1: Centralized Identity**



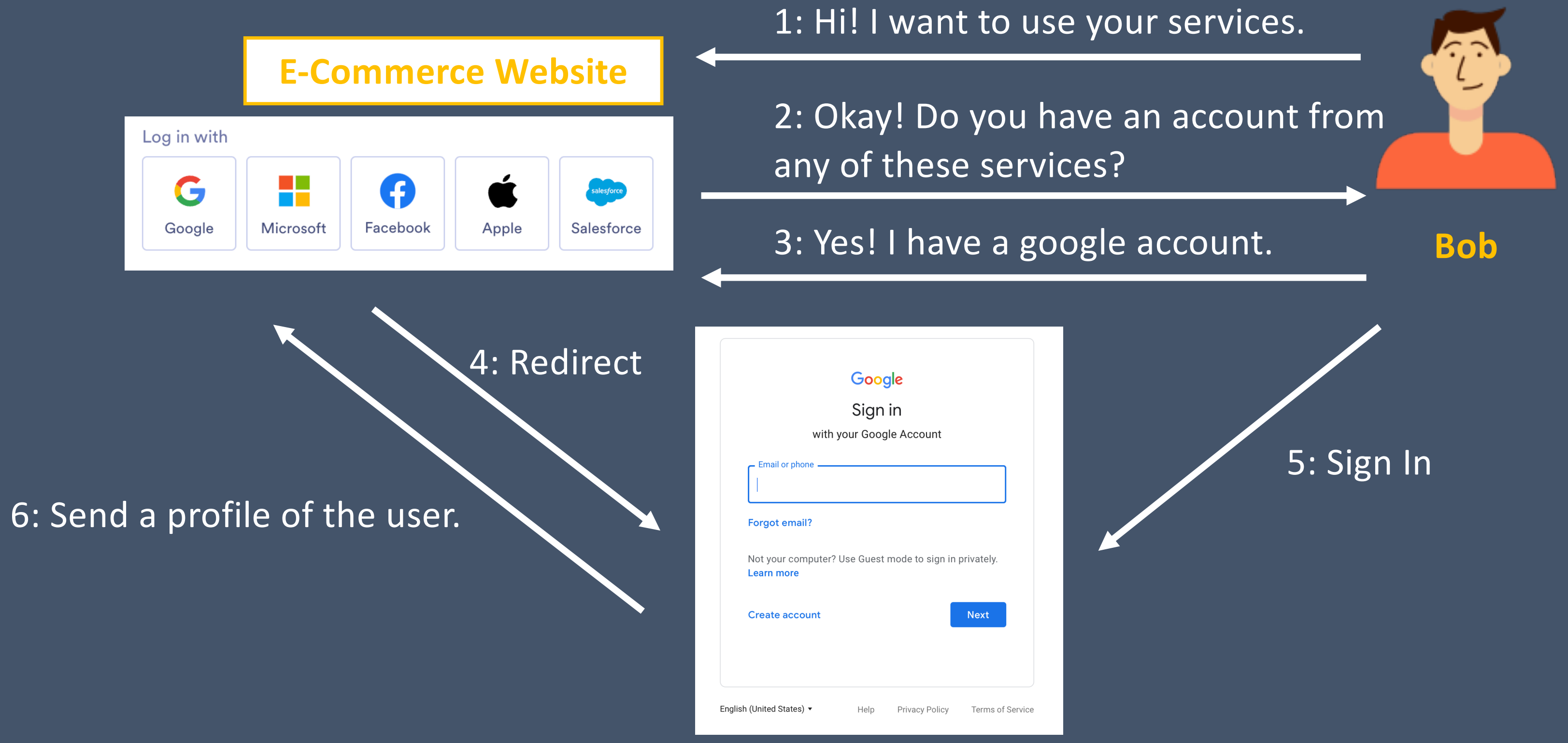
Identity and Access Management Systems

- **Phase 1: Centralized Identity**



Identity and Access Management Systems

- **Phase 2: Federated or User-Centric Identity**



E-Commerce Website

1: Hi! I want to use your services.

2: Okay! Do you have an account from any of these services?

3: Yes! I have a google account.

4: Redirect

5: Sign In

6: Send a profile of the user.

Google

Sign in

with your Google Account

Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more

Create account

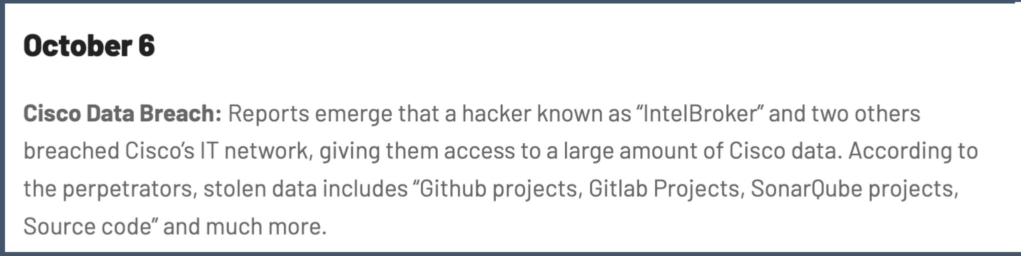
Next

English (United States) ▾ Help Privacy Policy Terms of Service

Issues with Early Phases of IAM Systems

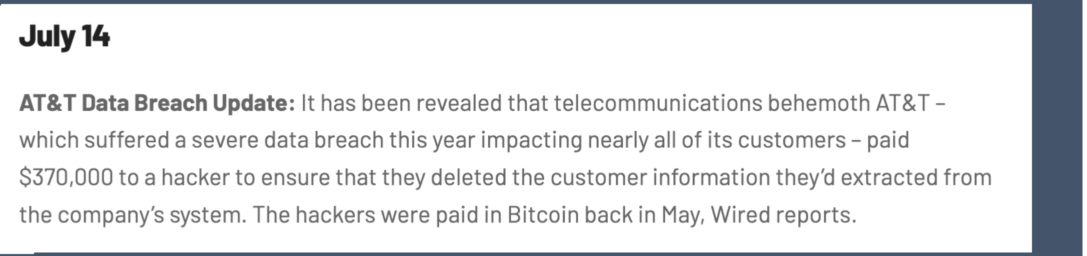
- During the centralized identity phase, user's identities are handled and manipulated by a central authority (e.g., ABC Company or the service provider).
- Also, during the federated identity phase, users must rely on the federated central authority to handle and manipulate their personal information or identities.

What will happen if they let your identities or personal information objects expose to unauthorized entities?



October 6

Cisco Data Breach: Reports emerge that a hacker known as "IntelBroker" and two others breached Cisco's IT network, giving them access to a large amount of Cisco data. According to the perpetrators, stolen data includes "Github projects, Gitlab Projects, SonarQube projects, Source code" and much more.



July 14

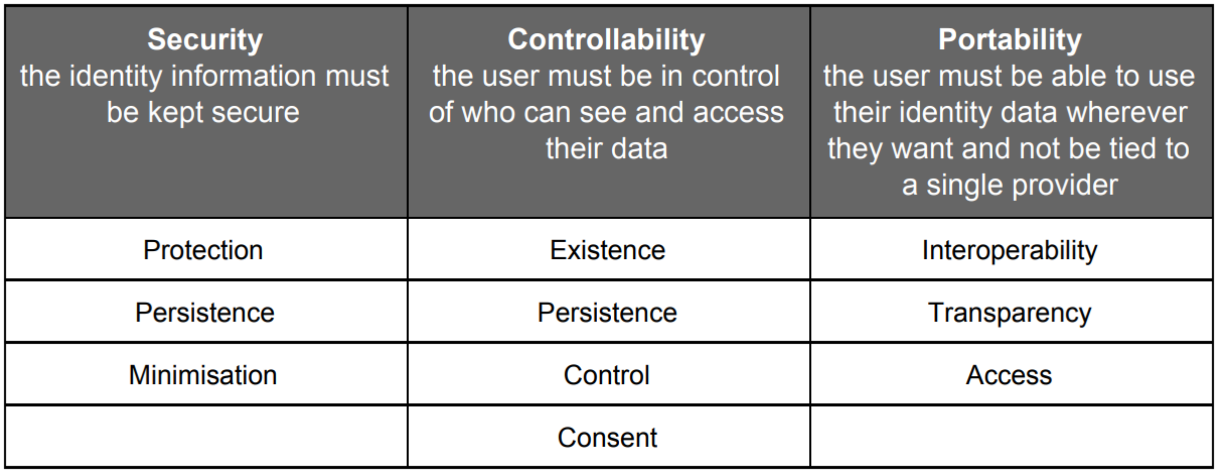
AT&T Data Breach Update: It has been revealed that telecommunications behemoth AT&T – which suffered a severe data breach this year impacting nearly all of its customers – paid $370,000 to a hacker to ensure that they deleted the customer information they'd extracted from the company's system. The hackers were paid in Bitcoin back in May, Wired reports.

Introduction to Decentralized Identity

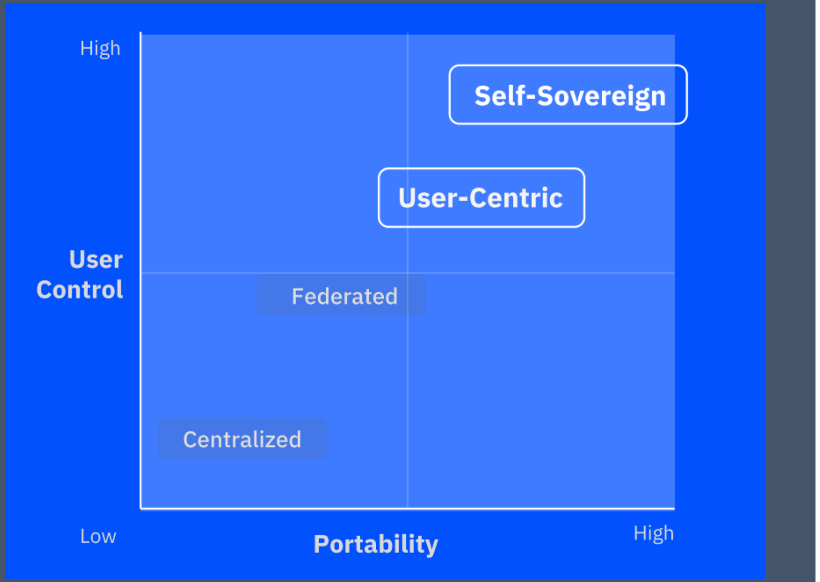
Self-Sovereign Identity, Verifiable Credentials, and Decentralized Identifiers.

What is Self-Sovereign Identity?

- Self-sovereign identity (SSI) can be defined as an identity of a person that is fully owned and controlled by the person. It is not dependent on or subject to any other authority or trusted third party. This is considered a decentralized identity.

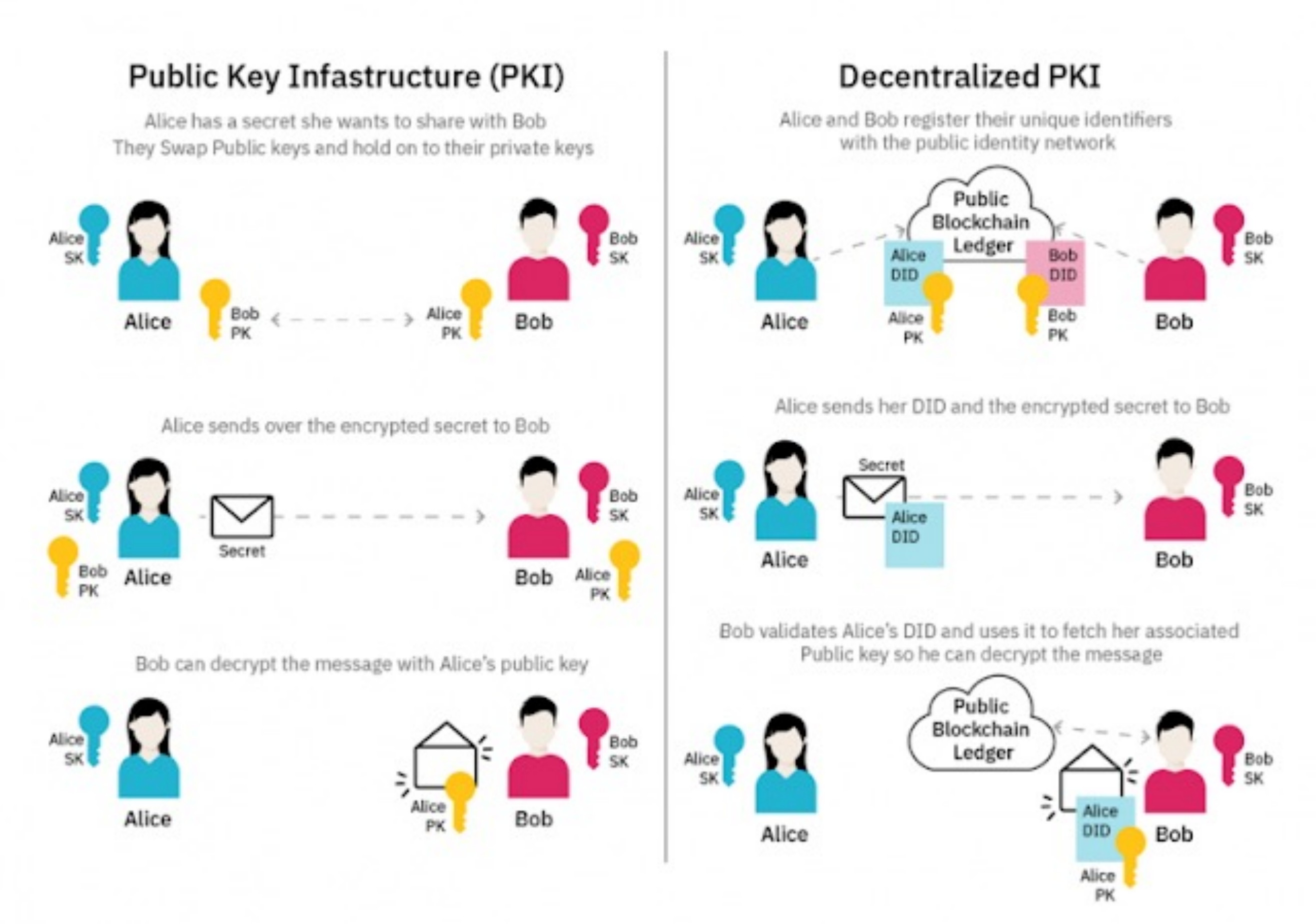


Security the identity information must be kept secure	**Controllability** the user must be in control of who can see and access their data	**Portability** the user must be able to use their identity data wherever they want and not be tied to a single provider
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	



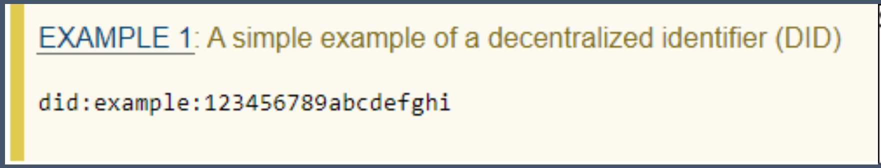
What is Self-Sovereign Identity?

- There are some basic terminologies that were used to build up the self-sovereign identity into actions.
  - **Decentralized Public Key Infrastructure (DPKI):** “It enables everyone to create or anchor cryptographic keys on the Blockchain in a tamper-proof and chronologically ordered way. ”


Public Key Infastructure (PKI)
Alice has a secret she wants to share with Bob
They Swap Public keys and hold on to their private keys
Alice SK
Alice
Bob PK
Alice PK
Bob
Bob SK
Alice sends over the encrypted secret to Bob
Alice SK
Bob PK
Alice
Secret
Bob
Alice PK
Bob SK
Bob can decrypt the message with Alice's public key
Alice SK
Alice
Alice PK
Bob
Bob SK
Decentralized PKI
Alice and Bob register their unique identifiers
with the public identity network
Alice SK
Alice
Public Blockchain Ledger
Alice DID
Alice PK
Bob DID
Bob PK
Bob
Bob SK
Alice sends her DID and the encrypted secret to Bob
Alice SK
Alice
Secret
Alice DID
Bob
Bob SK
Bob validates Alice's DID and uses it to fetch her associated
Public key so he can decrypt the message
Alice SK
Alice
Public Blockchain Ledger
Alice DID
Alice PK
Bob
Bob SK

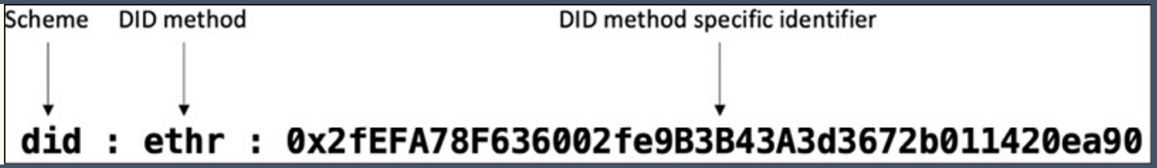
What is Self-Sovereign Identity?

- There are some basic terminologies that were used to build up the self-sovereign identity into actions.
  - **Decentralized Identifiers (DIDs):** “A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology (DLT) or other form of decentralized network. The generic format of a DID is defined in this specification. A specific DID scheme is defined in a DID method specification.” (W3C, 2016)



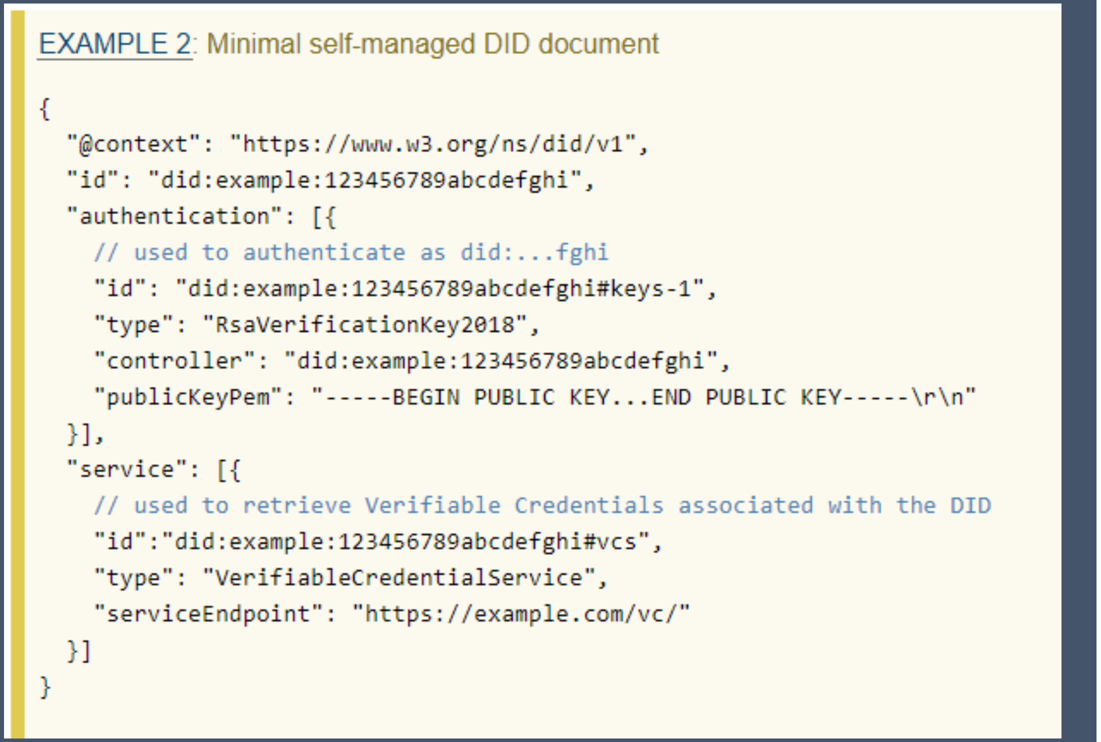
EXAMPLE 1: A simple example of a decentralized identifier (DID)

```
did:example:123456789abcdefghi
```


Scheme
DID method
DID method specific identifier
did : ethr : 0x2fEFA78F636002fe9B3B43A3d3672b011420ea90

What is Self-Sovereign Identity?

- There are some basic terminologies that were used to build up the self-sovereign identity into actions.
    - **DID Document:** “A set of data that describes the DID subject, including mechanisms, such as public keys and pseudonymous biometrics, that the DID subject can use to authenticate itself and prove their association with the DID. …” (W3C, 2016).



EXAMPLE 2: Minimal self-managed DID document

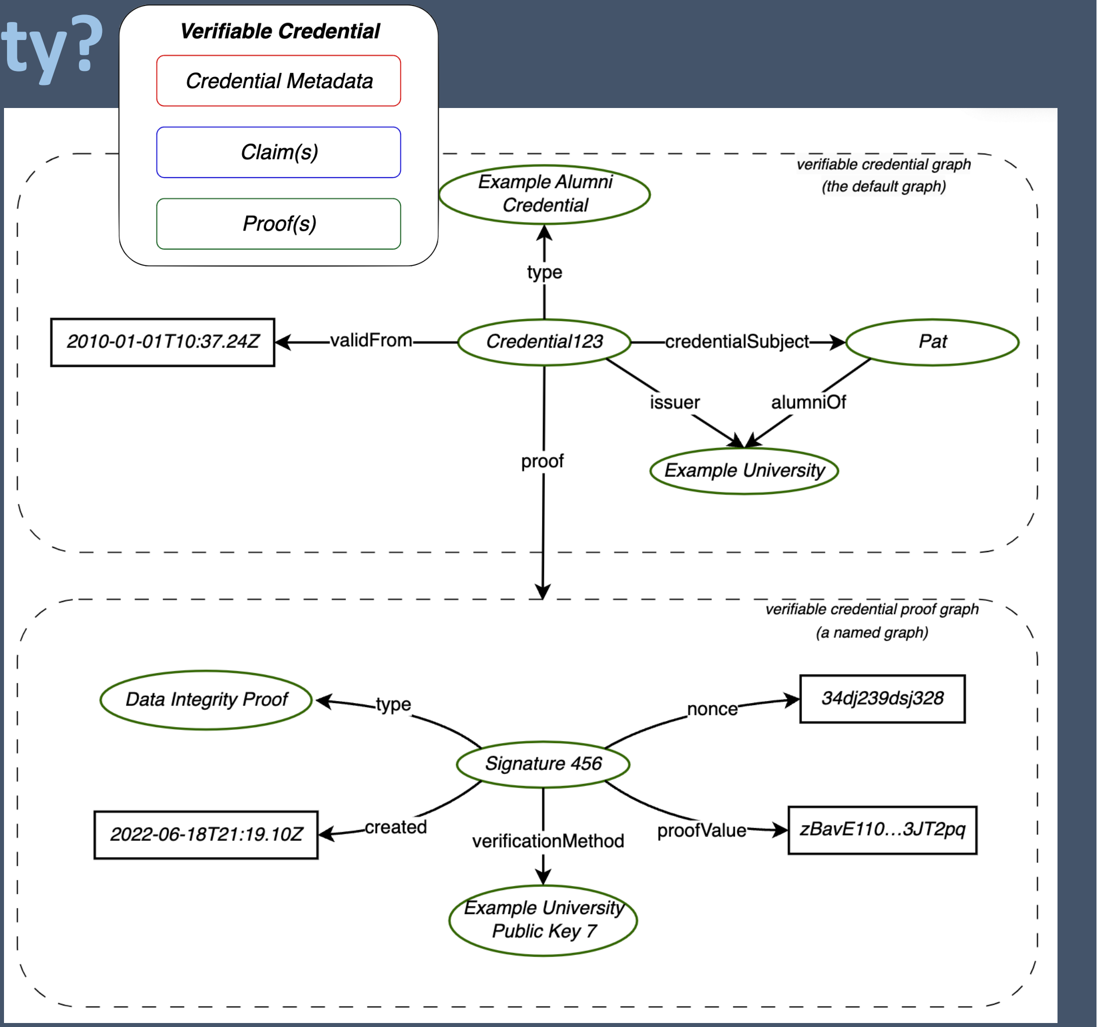
```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id":"did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

What is Self-Sovereign Identity?

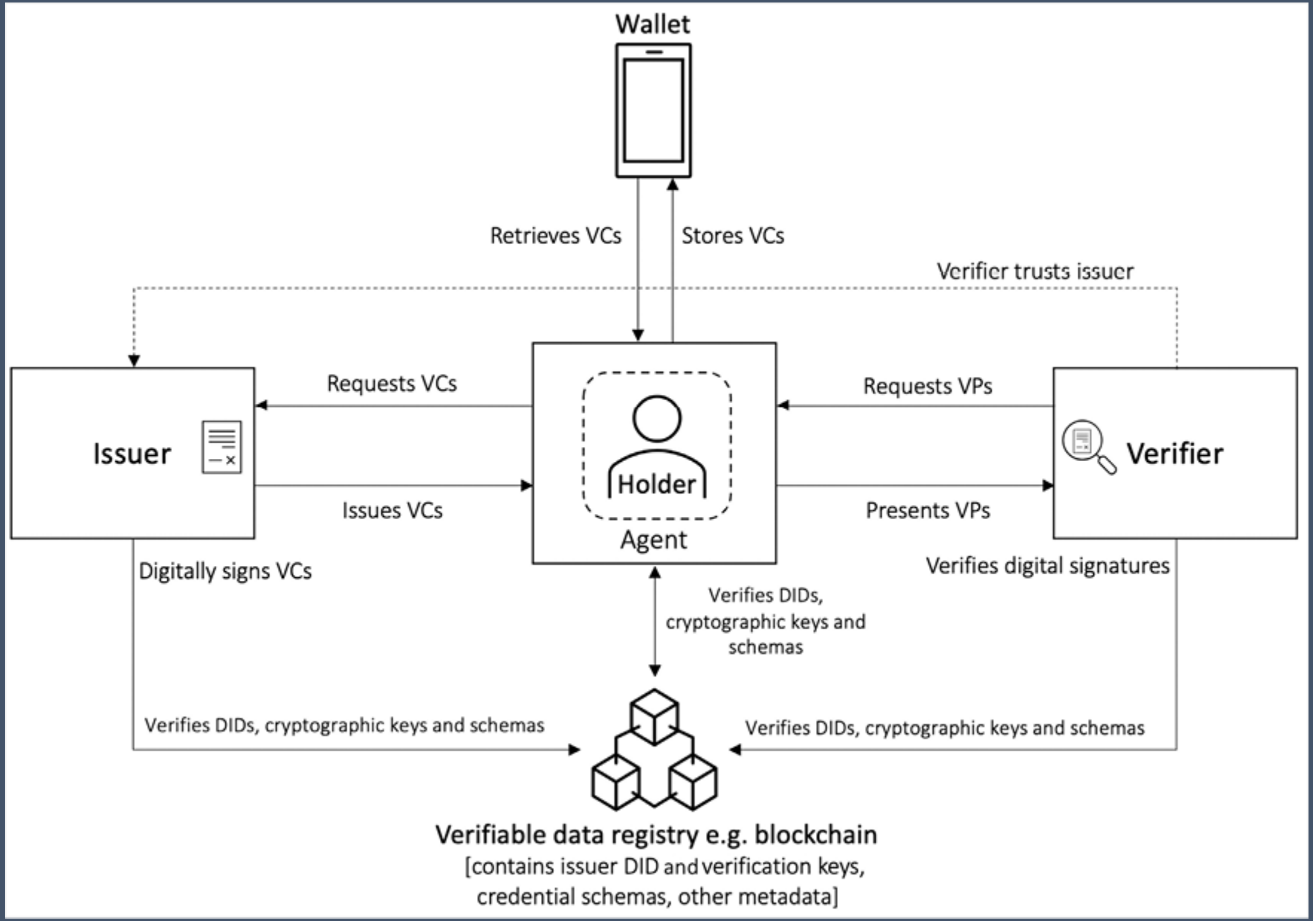
- There are some basic terminologies that were used to build up the self-sovereign identity into actions.
  - **Credentials:** A credential might consist of:
    - Information related to identifying the subject of the credential (for example, a photo, name, or ID number)
    - Information related to the issuing authority (for example, a city government, national agency, or certification body)
    - Information related to the type of credential (for example, a Dutch passport, an American driving license, or a health insurance card)
    - Information related to specific properties asserted by the issuing authority about the subject (for example, nationality, date of birth, or the classes of vehicle they're qualified to drive)
    - Evidence by which a subject was demonstrated to have satisfied the qualifications required for issuance of the credential (for example, a measurement, proof of citizenship, or test result)
    - Information related to constraints on the credential (for example, validity period, or terms of use).

What is Self-Sovereign Identity?

- There are some basic terminologies that were used to build up the self-sovereign identity into actions.
  - **Verifiable Credentials (VCs):** "A verifiable credential can represent all the same information that a physical credential represents. Adding technologies such as digital signatures can make verifiable credentials more tamper-evident and trustworthy than their physical counterparts." (W3C, 2024).



Verifiable Credential Eco-System


Wallet
Retrieves VCs
Stores VCs
Verifier trusts issuer
Issuer
Requests VCs
Issues VCs
Holder
Agent
Requests VPs
Presents VPs
Verifier
Digitally signs VCs
Verifies digital signatures
Verifies DIDs, cryptographic keys and schemas
Verifies DIDs, cryptographic keys and schemas
Verifies DIDs, cryptographic keys and schemas
Verifiable data registry e.g. blockchain
[contains issuer DID and verification keys, credential schemas, other metadata]

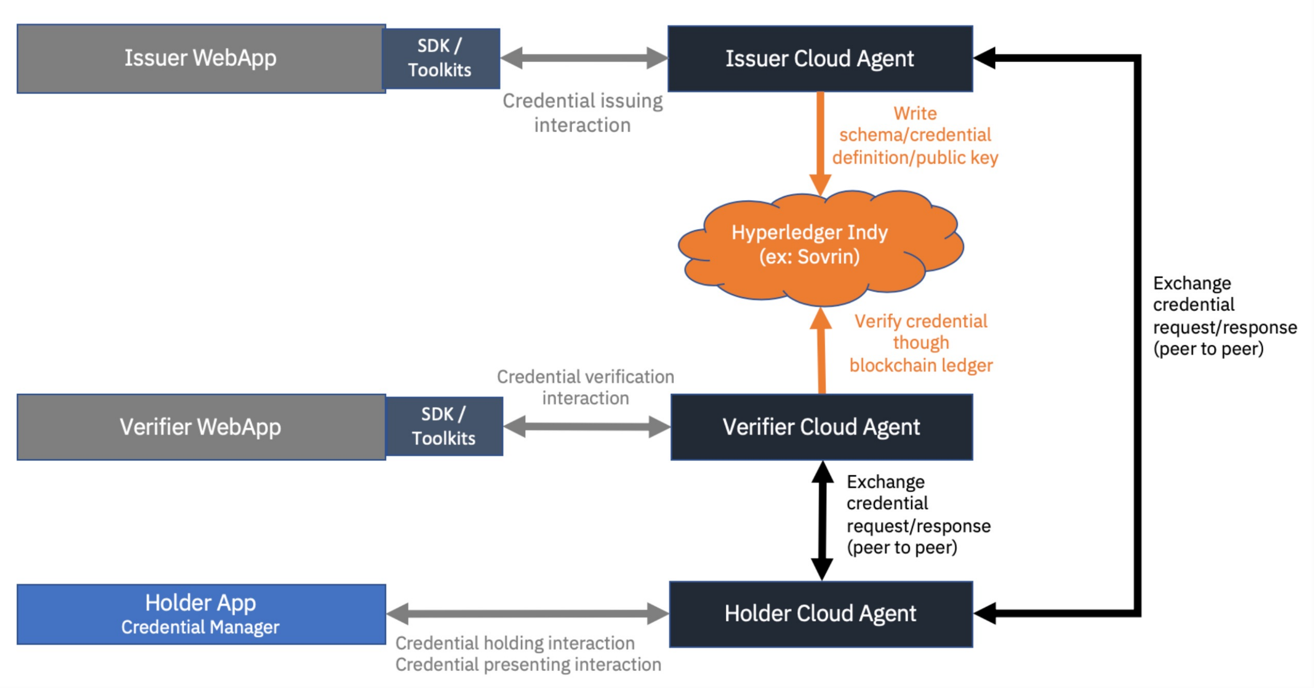
- **Issuer:** The entity that issues VCs to the subjects.
- Subject: An entity whose claims (attributes) are stored in the VC.
- **Holder:** An entity that is in possession of the VC and presents it to the verifier for verification as and when required.
- **Verifier:** An entity that ensures that the claims made in the VC are true and correct. The verifier receives VCs from the holder and verifies them.
- **Digital wallet:** An entity that stores the VCs for the holder.
- **Digital agent:** Software that acts as an interface between the VC ecosystem and the holder, e.g., an app on a mobile phone.
- **Verifiable data registry:** This is an entity that is the foundation of the VC ecosystem and decentralized identity ecosystem. Verifiable Data Registries (VDRs) can be blockchains or decentralized and centralized databases. However, blockchains, due to their inherent security features, can be more suitable in the decentralized identity ecosystem.

SSI-Specific Blockchain Projects

- The **Hyperledger identity stack** consists of Indy, Aries, Ursa, and AnonCreds, which are flexible and can interoperate with other layers in the SSI stack:
  - **Hyperledger Indy** was the Hyperledger foundation's first blockchain framework that targeted identity use cases. It is a public permissioned blockchain specifically built for decentralized identity use cases. It can build and publish DIDs, VCs, and other similar elements of the blockchain.
  - **Hyperledger Ursa** grew out of Hyperledger Indy as a separate project, which consists of cryptography components of Hyperledger Indy.
  - **AnonCreds** is another project that stems out of Indy. It is the ZKP-based VCs mechanism that has been extracted from Indy as a standalone project.
  - **Hyperledger Aries** is another project that spun out of Indy. It can be seen as the digital agent mechanism in the Hyperledger identity stack. Aries is an attempt to bridge DIDs and VCs from multiple SSI ecosystems. Aries enables DID-oriented messaging between agents and uses some protocols to enable the issuance, presentation, and verification of VCs.

SSI-Specific Blockchain Projects

- **Hyperledger Indy** was the Hyperledger foundation’s first blockchain framework that targeted identity use cases. It is a public permissioned blockchain specifically built for decentralized identity use cases. It can build and publish DIDs, VCs, and other similar elements of the blockchain.

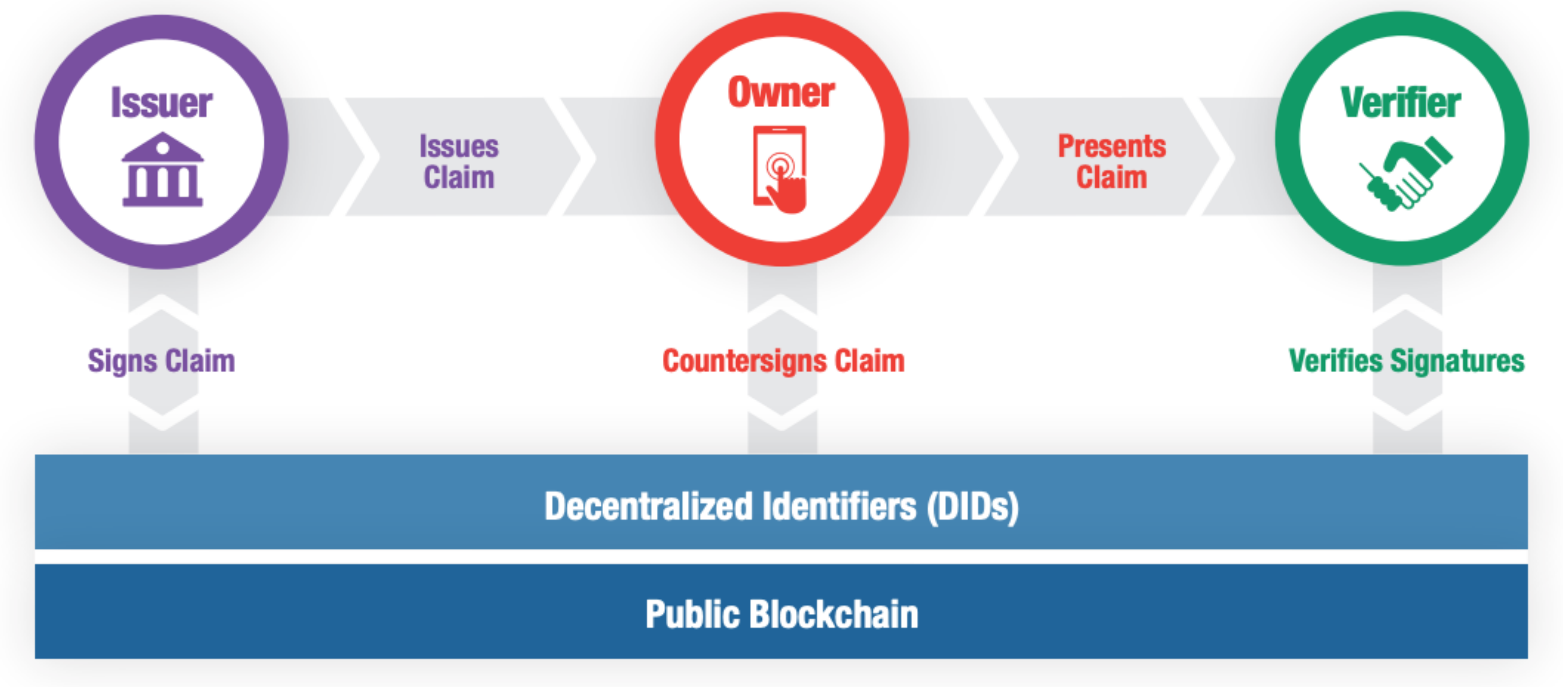

Issuer WebApp
SDK / Toolkits
Credential issuing interaction
Issuer Cloud Agent
Write schema/credential definition/public key
Hyperledger Indy (ex: Sovrin)
Verify credential though blockchain ledger
Exchange credential request/response (peer to peer)
Credential verification interaction
Verifier WebApp
SDK / Toolkits
Verifier Cloud Agent
Exchange credential request/response (peer to peer)
Holder App
Credential Manager
Holder Cloud Agent
Credential holding interaction
Credential presenting interaction

SSI-Specific Blockchain Projects

- **Other projects:**
  - **KILT:** KILT is a decentralized blockchain protocol for issuing VCs and DIDs for Web3.
  - **Proof of Humanity:** This project aims to thwart sybil attacks by utilizing social verification with video submission to allow users to prove that they are real humans.
  - **uPort:** This platform allows users to create a portable, reusable, and decentralized digital identity that can be used across different services. The identity is a smart contract on the Ethereum blockchain as a digital representation of the user.
  - **Sovrin:** This is a public service utility that enables SSI on the internet.

SSI-Specific Blockchain Projects

- **Other projects:**
  - **Sovrin:** This is a public service utility that enables SSI on the internet.



Challenges of Decentralized Identity

- Some challenges need to be addressed to further improve the SSI ecosystem:
  - **Lost device** – What if a device (mobile phone) on which all of a person's VCs are stored is stolen or left behind on a train?
  - The **transition from web 2.0 to Web 3.0** poses some challenges, in terms of migration of data, accounts, etc. from web 2.0 to Web 3.0.
  - **Digital wallet vulnerabilities** – As the device on which the wallet is hosted and the wallet itself are subject to *malware* and *hacking* attacks, it's important to ensure that the wallets are tested thoroughly before public release
  - Other challenges include limitations on the VDR/blockchain layer, such as privacy, scalability, and interoperability.

Today’s Agenda

- Upon successful of today’s lecture, you have learned about:
    - Detailed Background on Identity and Access Management System from a story between centralized identity, federated identity, and decentralized identity.
    - The problem with Centralized Identity and its Evolution, such as the need of central authority and data leakage.
    - Decentralized Identity and Self-Sovereign Identity, including the verifiable credentials, and decentralized identifiers.

End of the lecture! 🥳

Please feel free to ask any questions.

If you need further discussion, please contact me:

- Email me at charnon@cmkl.ac.th
- Appoint me for 1-on-1 discussion during the office hours.