

# Decentralized Identity Management & SSI

Öz, B., Hoops, F., Gebele, J., & Matthes, F. (2024). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Chair of Software Engineering for Business Information Systems (sebis)  
Department of Computer Science  
School of Computation, Information and Technology (CIT)  
Technical University of Munich (TUM)  
[www.matthes.in.tum.de](http://www.matthes.in.tum.de)

## 1. Introduction

- Today's Digital Identity
- Problems with Today's Digital Identity
- Identity Paradigms
- Diploma Use Case

## 2. Self-Sovereign Identity

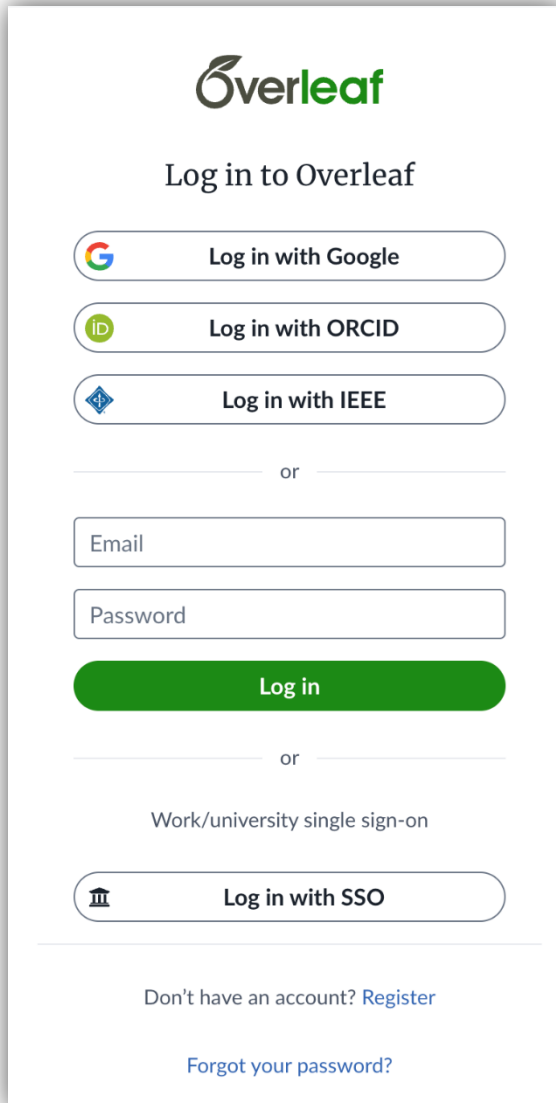
- Motivation
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers
- Protocols

## 3. SSI Use Cases

- Diploma Use Case
- Examples of SSI Usage

## 4. Challenges

- SSI Criticism
- Challenges



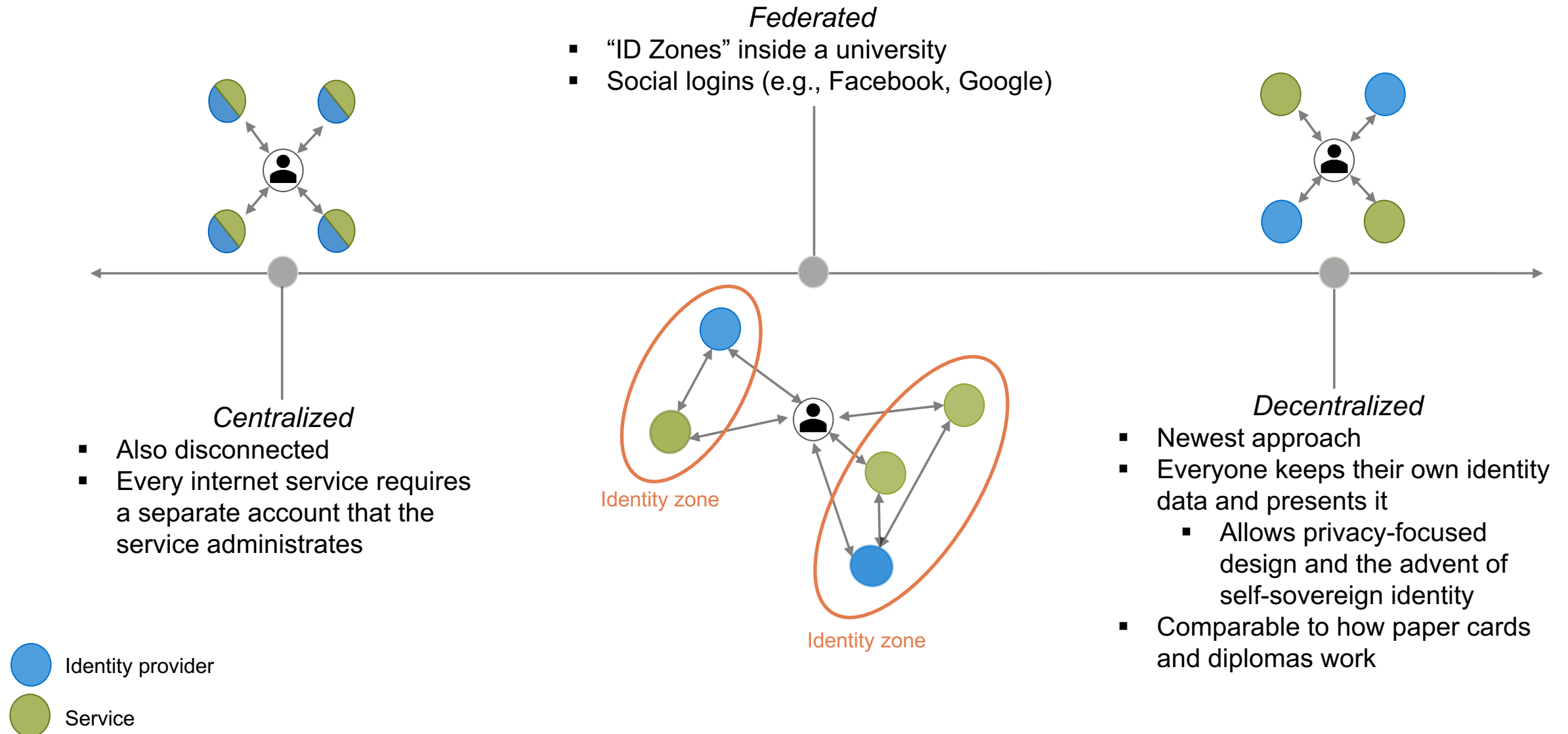
The screenshot shows the Overleaf login interface. At the top is the Overleaf logo. Below it is the text 'Log in to Overleaf'. There are three buttons for federated login: 'Log in with Google' (with the Google logo), 'Log in with ORCID' (with the ORCID logo), and 'Log in with IEEE' (with the IEEE logo). Below these is a horizontal line with the word 'or' in the center. Underneath are two input fields for 'Email' and 'Password', followed by a green 'Log in' button. Another horizontal line with 'or' follows. Below that is the text 'Work/university single sign-on' and a button 'Log in with SSO' (with a building icon). At the bottom, there are two links: 'Don't have an account? Register' and 'Forgot your password?'.

*Screenshot illustrating federated logins.*

- In the digital age, we need digital identity for offline and online services.
- Sometimes, a pseudonymous identity, such as an email, is sufficient, and other times, we need our natural identity:
  - Social media accounts usually just require an email address
  - Banking requires natural identity verification for regulatory reasons
- Everyone effectively has multiple identities, for example, for work, and for personal use.
- Identity in its purest form can be viewed as a collection of claims about an identifier.
- An identity paradigm dictates the way identity is managed and used.
  - The Internet primarily relies on **federated identity management**.

- Centralization of User Data
  - Big tech monopolies have a lot of user data in centralized databases, which are prone to high-impact data breaches.
  - These big identity providers also sell user data, sometimes violating laws in the user's country.
- Reliance on Passwords
  - Federated identity systems require users to remember passwords, leading to security breaches due to weak and reused passwords.
- Big Identity Providers are Gatekeepers
  - Arbitrary account suspension locks users out of their accounts with other services.
  - Censorship or outages can prevent users from using all connected services.

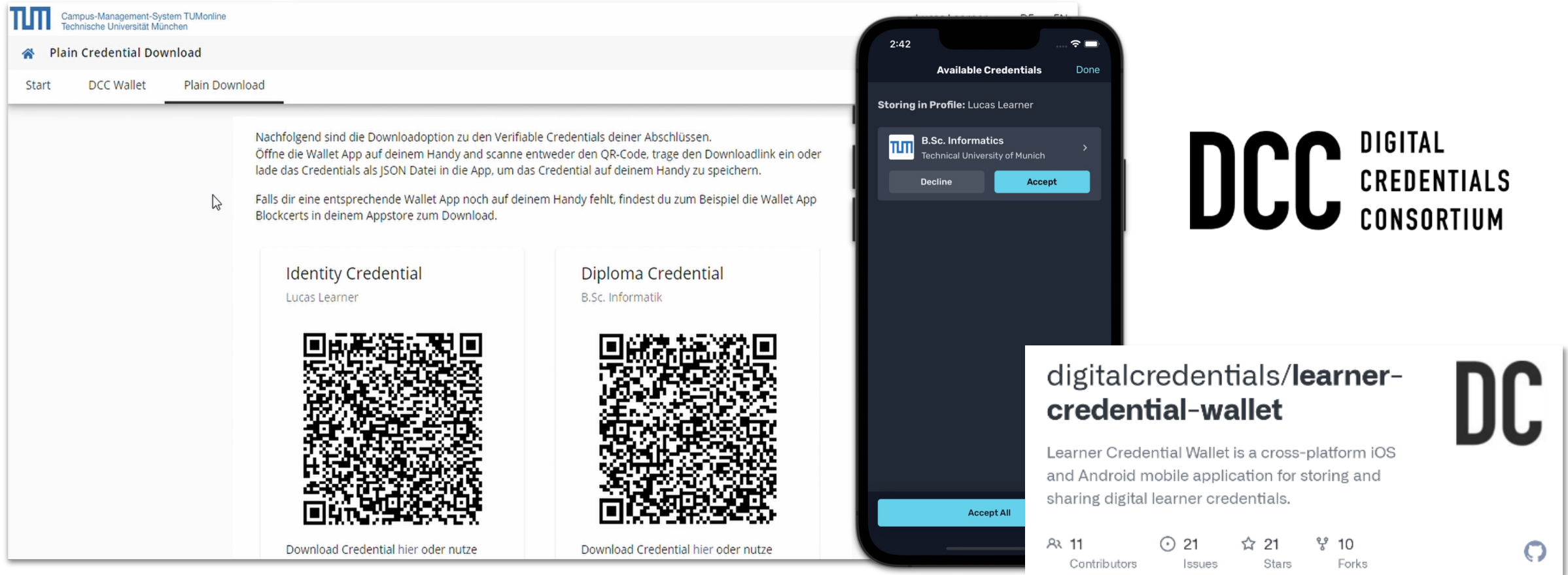
In order to tackle these issues, there should be a move towards decentralized identity management (IDM) solutions that empower users with control over their identity information and allow for interoperability among various systems.





# Decentralized Identity Use Case Preview: Diplomas

Students can receive a diploma credential from their university and save it to their mobile wallet.



The image displays a web interface for downloading credentials from TUMonline and a mobile app interface for the Digital Credentials Consortium (DCC) wallet.

**Web Interface (TUMonline):**

- Header: TUM Campus-Management-System TUMonline Technische Universität München
- Section: Plain Credential Download
- Navigation: Start, DCC Wallet, Plain Download
- Instructions: "Nachfolgend sind die Downloadoption zu den Verifiable Credentials deiner Abschlüssen. Öffne die Wallet App auf deinem Handy und scanne entweder den QR-Code, trage den Downloadlink ein oder lade das Credentials als JSON Datei in die App, um das Credential auf deinem Handy zu speichern. Falls dir eine entsprechende Wallet App noch auf deinem Handy fehlt, findest du zum Beispiel die Wallet App Blockcerts in deinem Appstore zum Download."
- Credentials for Download:
  - Identity Credential** (Lucas Learner): QR code and link "Download Credential hier oder nutze".
  - Diploma Credential** (B.Sc. Informatik): QR code and link "Download Credential hier oder nutze".

**Mobile App Interface:**

- Header: Available Credentials Done
- Section: Storing in Profile: Lucas Learner
- Credential: B.Sc. Informatics Technical University of Munich
- Buttons: Decline, Accept
- Bottom Button: Accept All

**DCC Digital Credentials Consortium:**

- Logo: DCC
- Text: DIGITAL CREDENTIALS CONSORTIUM

**digitalcredentials/learner-credential-wallet:**

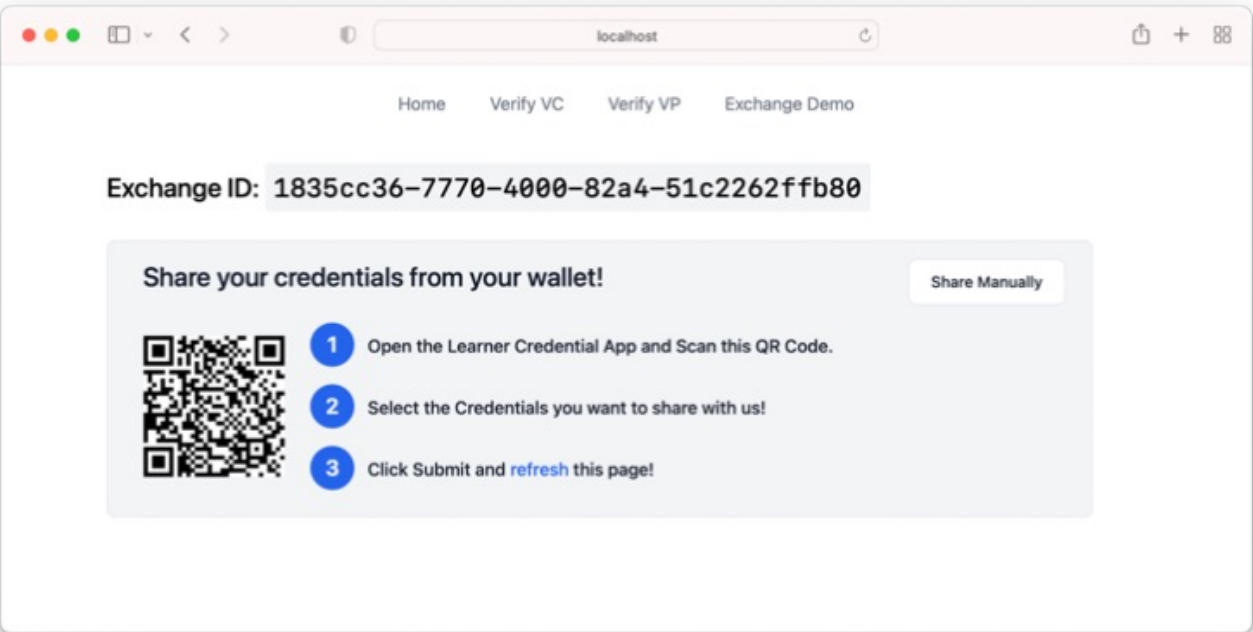
- DC
- Description: Learner Credential Wallet is a cross-platform iOS and Android mobile application for storing and sharing digital learner credentials.
- Stats: 11 Contributors, 21 Issues, 21 Stars, 10 Forks

# Decentralized Identity Use Case Preview: Diplomas (cont.)

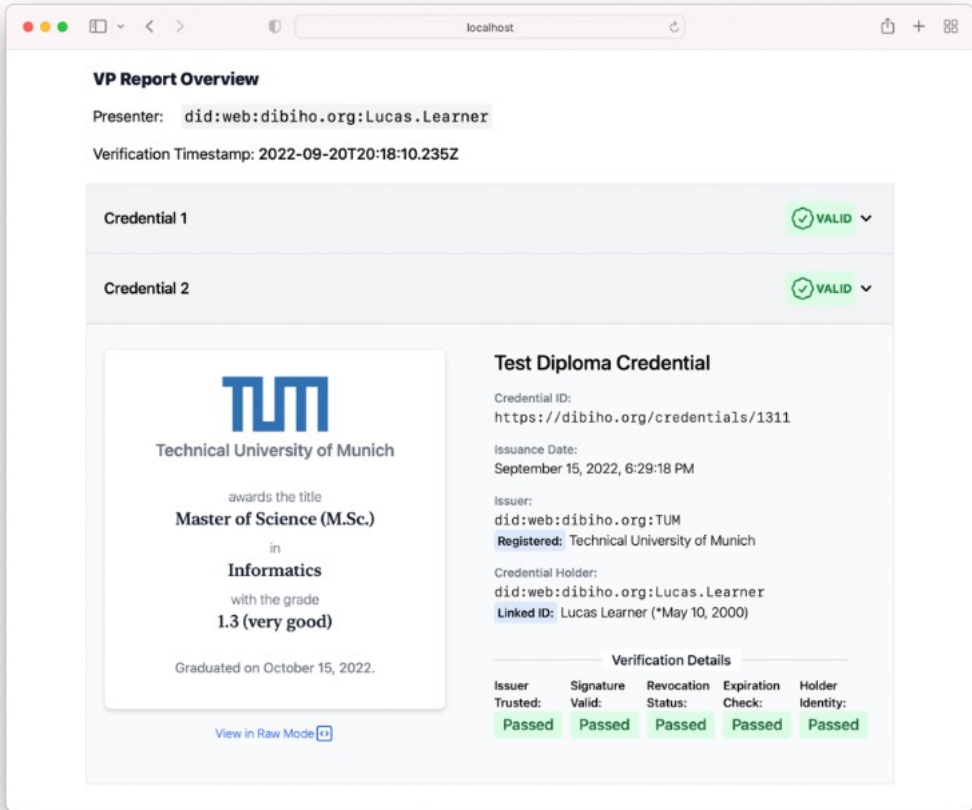


Example:  
You want to present your MSc Certificate in Computer science to a potential employer.

Your view:



Employer view:



## 1. Introduction

- Today's Digital Identity
- Problems with Today's Digital Identity
- Identity Paradigms
- Diploma Use Case

## 2. Self-Sovereign Identity

- Motivation
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers
- Protocols

## 3. SSI Use Cases

- Diploma Use Case
- Examples of SSI Usage

## 4. Challenges

- SSI Criticism
- Challenges



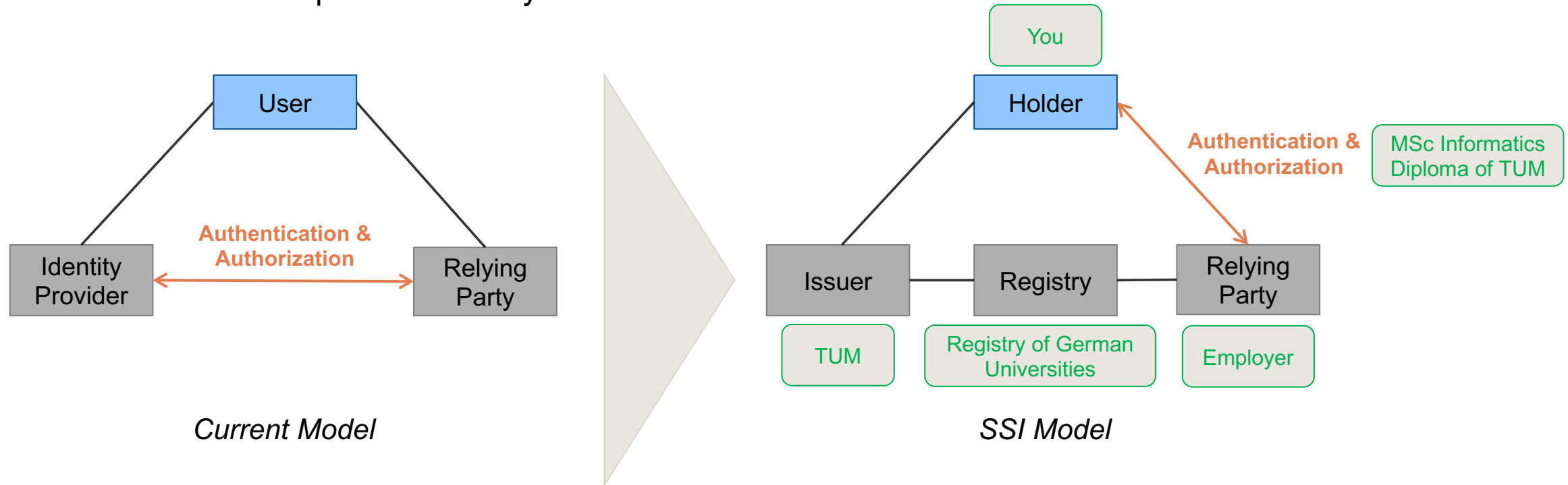
# Motivating Self-Sovereign Identity (SSI)

- Today's identity providers have immense amounts of power over us and metadata about us.
- Offline, you receive a state-issued ID card that you and only you control after issuance:
  - You decide when and to whom you identify yourself.
  - Everyone accepts your ID card.
  - No one can prevent you from physically presenting your ID card.
  - The act of physically presenting an ID card is not trackable by any third party.

We should strive to make **online identity better than paper-based identity across the board**. Digitalization should not just be about making a process faster but should also retain important properties of the old process.

## The Motivation Behind SSI (cont.)

- **Self-Sovereign Identity** (SSI) is the term used to describe this target architecture.
- With SSI you can instantly create an account (i.e., identifier) without anyone being able to prevent it.
  - You alone control that account, which means no one can shut it down or take it over.
  - The account is compatible with any online service.



As we will see, **blockchain technology** is a solid choice to publish and administrate such an account.

According to Christopher Allen<sup>1</sup>, the concept of Self-Sovereign Identity (SSI) originated in the early 90s. The idea was first introduced in the PGP's 'Web of Trust' in 1991, which showcased a decentralized trust management system for email addresses.

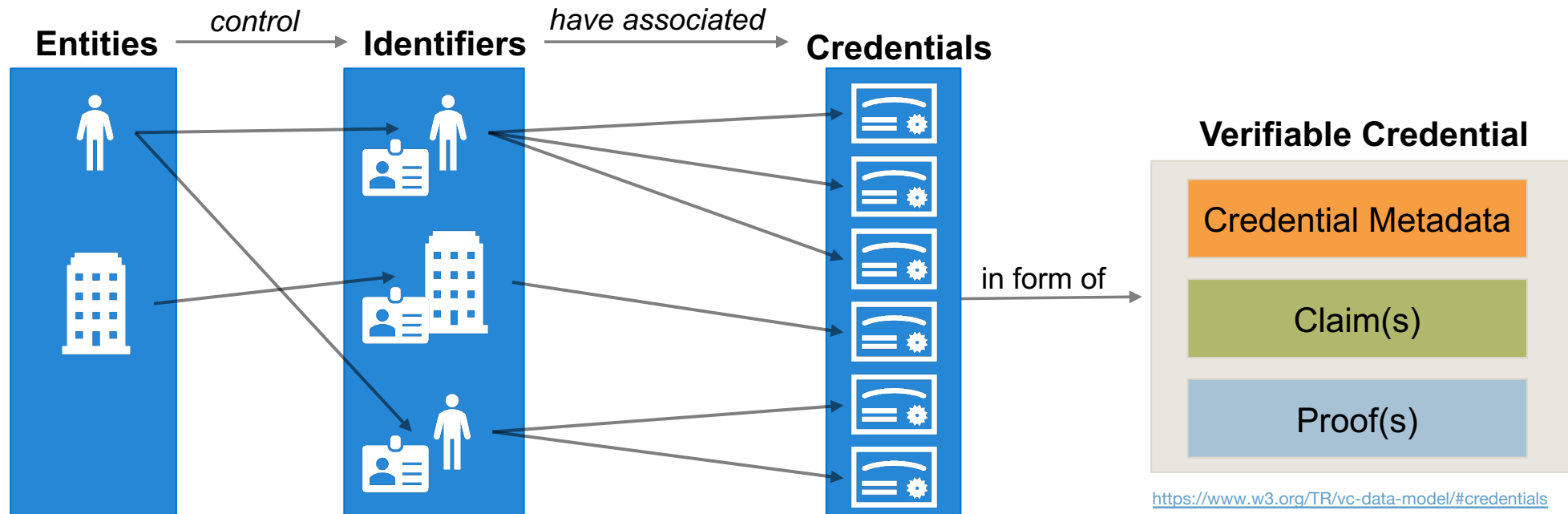
Christopher Allen has had a significant role in coining the term SSI. He identified **ten core principles**<sup>1</sup>:

- 1) **Inclusion:** Identity should be available to all
- 2) **Control:** Users must control their own identities
- 3) **Access:** Users must have access to their own data
- 4) **Transparency:** Systems and governance must be transparent
- 5) **Persistence:** Identities must be long-lived
- 6) **Portability:** Identity information and services must be transportable
- 7) **Interoperability:** Identities should be as widely usable as possible
- 8) **Consent:** Users must agree to the use of their identity or data
- 9) **Minimization:** Disclosure of identity information must be minimized
- 10) **Protection:** Users' right to privacy must be protected<sup>4</sup>

<sup>1</sup><http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>

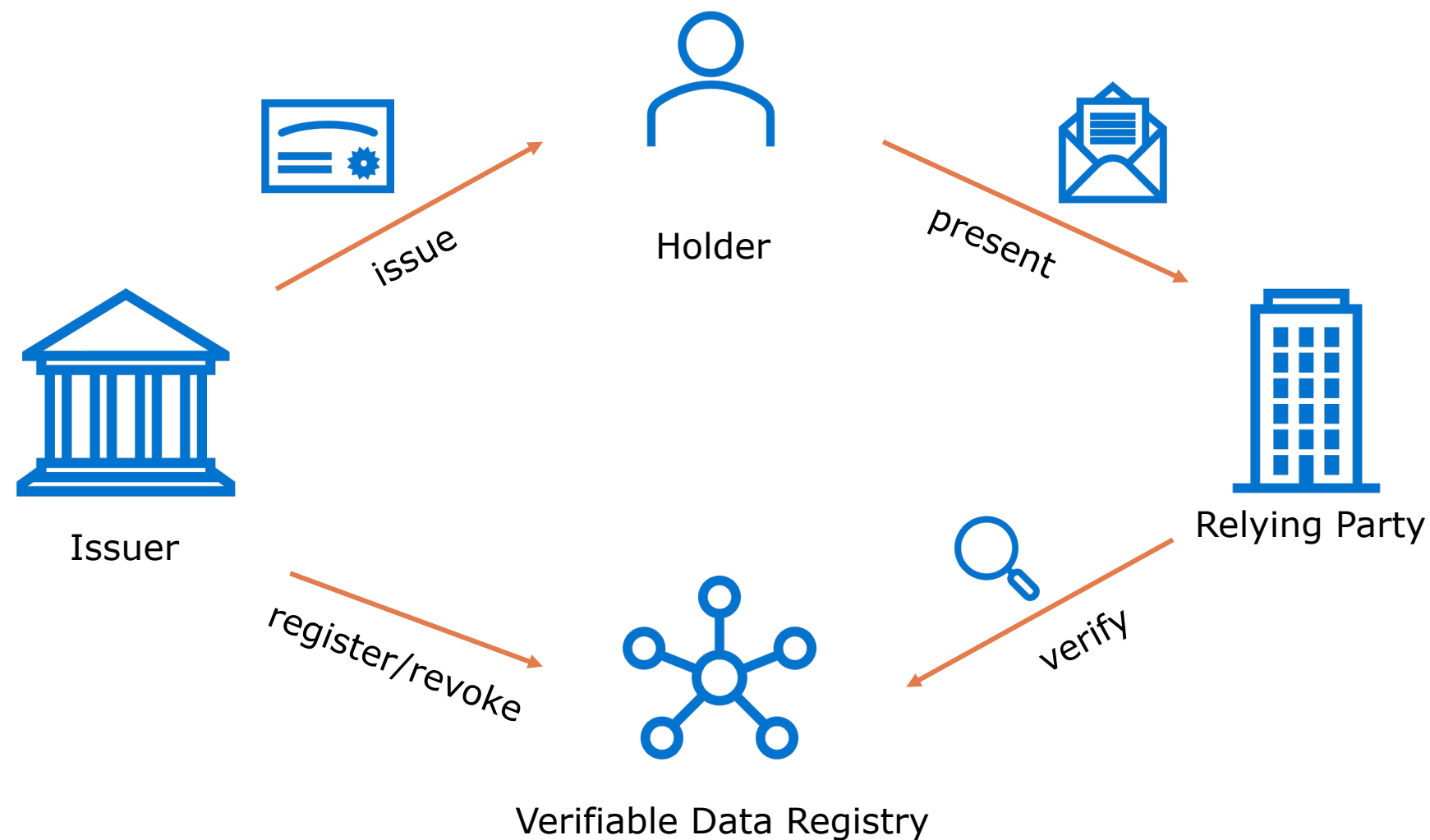
# Rough SSI Definition

- Self-Sovereign Identity (SSI) is still a very new approach, and definitions vary slightly.
- Rough definition:
  - It is a model in which entities are represented by digital identities, and every entity has **sole ownership** over the ability to control their identity data.
  - An identity can be seen as an account consisting of a pseudonymous identifier and an arbitrary number of attributes that are confirmed by some witness.
  - It is a paradigm that emphasizes privacy. Entities can decide what attributes to present to whom.



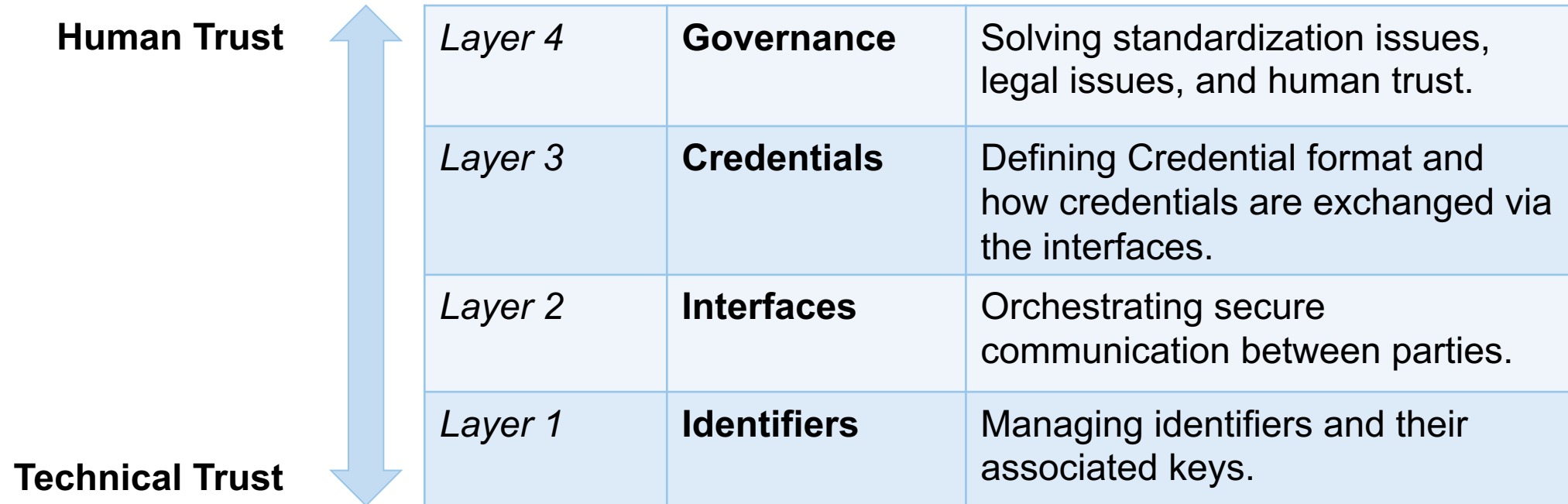
<https://www.w3.org/TR/vc-data-model/#credentials>

# Lifecycle of a Verifiable Credential





Preukschat and Reed<sup>1</sup> propose a four-layer technology stack for SSI that goes from technical trust to human trust:



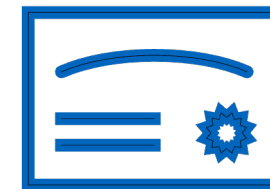
Adopting SSI for a use case means that challenges on all of these layers must be addressed. It is by no means only a technical problem.

<sup>1</sup><https://livebook.manning.com/book/self-sovereign-identity/chapter-5/v-8/8>

The World Wide Web Consortium (W3C), which creates guidelines and standards for the Internet, developed two core specifications for SSI:



- **Decentralized Identifier (DID):** A DID is a globally unique identifier for every entity in the SSI ecosystem. It does not need the use of a centralized authority. An example of a DID is *did:example:123456abcdef*.
- **Verifiable Credential (VC):** A VC is a means of making verifiable claims about an identity. This can be a government authority stating that a DID belongs to a certain Person's Name, Date of Birth, etc. But it could also be an entry pass for a building. Or a diploma.



# Decentralized Identifier Examples

A DID has the following structure:

<b>did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a</b>		
<b>Scheme</b> This part is static.	<b>Method</b> Usually short and identifies one specific publicly documented DID method. This one provides high decentralization and a low barrier to entry.	<b>Method-Specific Identifier</b> Arbitrarily long identifier. In this case, it is an Ethereum account address. Creating one is as easy as creating an Ethereum account.
<b>did:web:tum.de</b>		
<b>Scheme</b> This part is static.	<b>Method</b> Usually short and identifies one specific publicly documented DID method. This one enables easy adoption for institutions via an existing web presence.	<b>Method-Specific Identifier</b> Arbitrarily long identifier. In this case, it is a domain hosting a DID document at default relative path “/.well-known/did.json”.

DIDs are very flexible due to their reliance on **custom DID methods**. A custom DID method defines how to

- **create** an identifier
- **retrieve** information about the identifier (i.e., resolving to a DID document)
- **update** and **delete** information about the identifier (optional)

# Resolution of Decentralized Identifiers to DID Documents

- Decentralized Identifiers (DIDs) are unique identifiers created and controlled by the individual, organization, or device they identify, rather than being issued and controlled by a central authority.

## DID Resolution:

- A DID **resolver** is software that resolves a DID into a DID document by following a pre-defined algorithm specific to the DID's method.
- The resolution process may depend on external data sources like a blockchain.

## DID Document:

- 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.

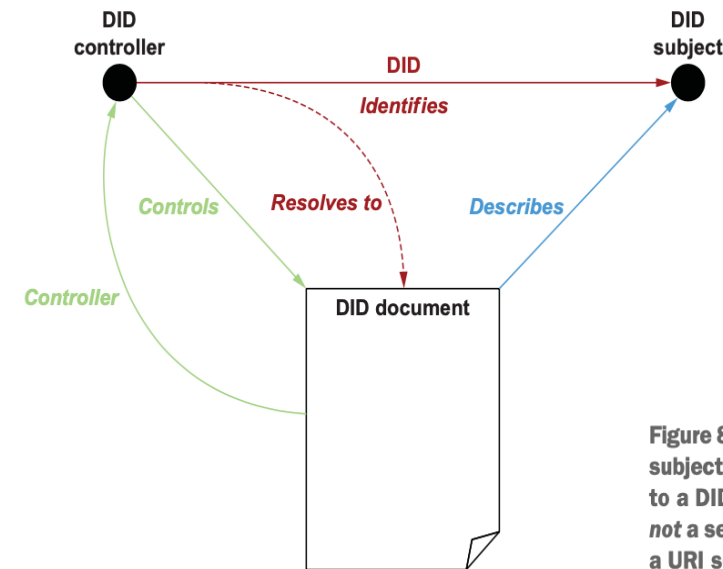


Figure 8.29 A DID always identifies a DID subject (whatever it may be) and resolves to a DID document. The DID document is *not* a separate resource and does *not* have a URI separate from the DID.

Image source: <https://www.w3.org/TR/did-core/>

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.

# Verifiable Credentials

- **Verifiable Credential:**

A Verifiable Credential (VC) is a digital representation of a set of claims that a third party can verify without needing a trusted intermediary. The key elements of a verifiable credential are:

**Credential Metadata:** Issuer as well as information about the format and purpose of the credential.

**Credential Claims:** Credential Subject and claims about the subject made by the issuer.

**Credential Proof:** A digital signature produced by the issuer that enables the credential to be verified by a third party.

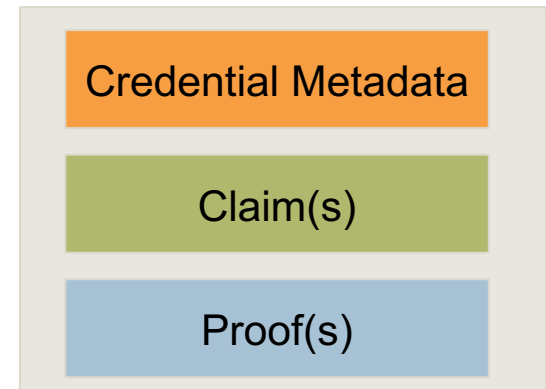
VCs can theoretically work with different types of identity. However, DIDs are the preferred solution to identify issuer, subject, and potential other involved entities.

- **Verifiable Presentation:**

A Verifiable Presentation (VP) is data derived from one or more Verifiable Credentials issued by one or more issuers that is specifically compiled for and shared with a specific verifier.

- Holders of VCs can generate VPs and then share these with verifiers to prove specific claims regarding their identity.
- A VP is signed by the holder and includes a nonce for replay protection.

## Verifiable Credential



<https://www.w3.org/TR/vc-data-model/#credentials>



# Verifiable Data Registry

Unlike centralized identity systems, the identities of the users are stored in each user's wallet.<sup>1</sup> However, there is still a need for publicly accessible data storage to support an SSI ecosystem. It needs to store and provide data to enable the following distinct functionalities:

## 1. Status Lists

- Support the revocation or suspension of credentials.

## 2. DID Documents

- Depends on the DID method used.

## 3. Trusted Issuer List

- One or more lists created by trust anchors that designate trustworthy issuers.

## 4. Logging (optional)

- Provides auditability (e.g., to detect fraudulent activity).

Different implementations can be used for each of these functionalities. Thus, the Verifiable Data Registry is a concept and not necessarily one single infrastructure.

The publicly readable Verifiable Data Registry should never expose private information (e.g., credentials themselves). **Data stored there is typically minimal, such as serial numbers or hashes of credentials.** Exact data and data structure are implementation-specific.

Using **blockchain technology as storage** can make sense because:

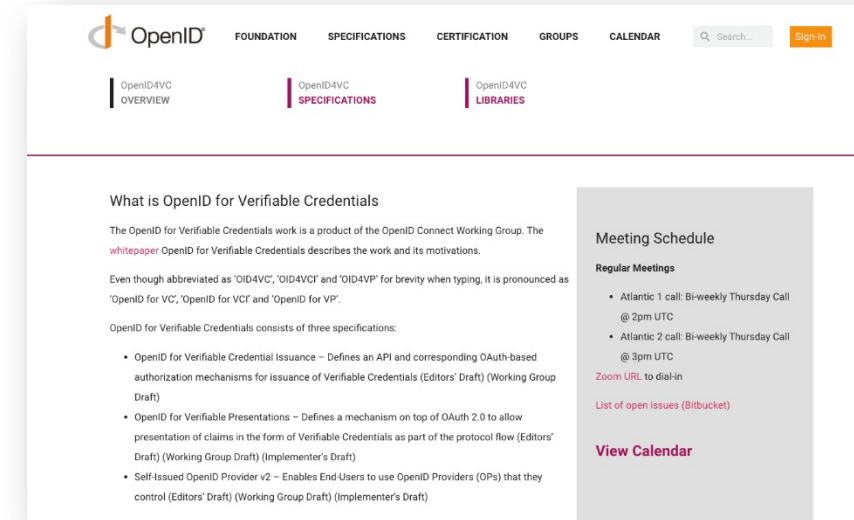
- It eliminates the need for participants to run server infrastructure
- It improves/creates transparency and auditability
- It provides reliable timestamping (relevant for issuance logging)

<sup>1</sup>Similar to a physical wallet, an SSI digital wallet stores your Verifiable Credentials and your DIDs.

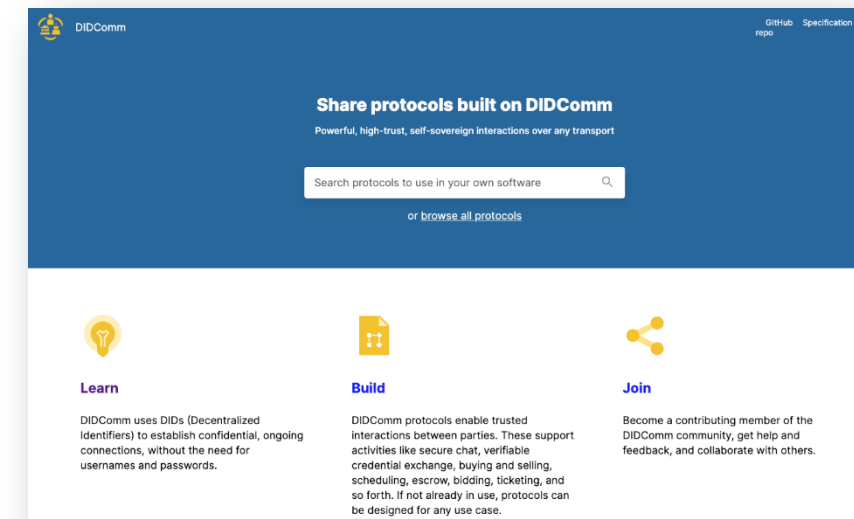
# Protocols for Verifiable Credential Exchange

- Issuance and presentation processes need standardized protocols
- There are two fundamental approaches:
  - Client-server
    - Web-based exchange via HTTP
    - *Example: OID4VC*
  - Peer-2-peer
    - Direct and symmetric message exchange
    - *Example: DIDComm*

Protocols for Verifiable Credential exchange have been developed, and there are very different philosophies behind them. For truly interoperable SSI, everyone must support the same set of protocols.



<https://openid.net/sg/openid4vc/>



<https://didcomm.org/>

## 1. Introduction

- Today's Digital Identity
- Problems with Today's Digital Identity
- Identity Paradigms
- Diploma Use Case

## 2. Self-Sovereign Identity

- Motivation
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers
- Protocols

## 3. SSI Use Cases

- Diploma Use Case
- Examples of SSI Usage

## 4. Challenges

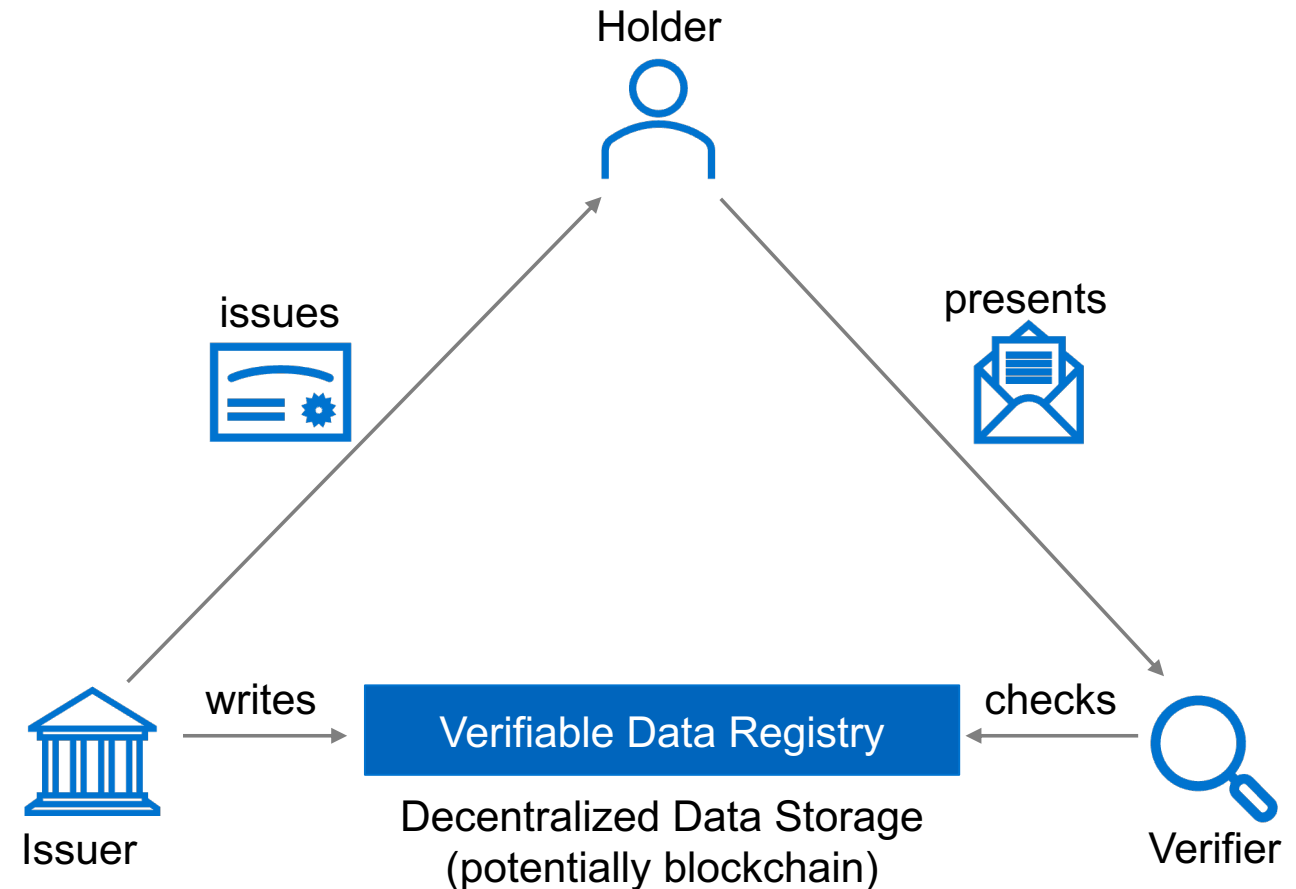
- SSI Criticism
- Challenges

Universities issue digital diplomas in the form of VCs. This provides students with a convenient and secure way to access and share their academic achievements with other institutions, prospective employers, or anyone else they want to.

Stakeholder	SSI Ecosystem Role	Comment
University	Issuer	Issues diplomas to students.
Student	Subject & Holder	Stores their diploma and keeps it on hand to present for job applications.
Company	Relying Party	Verifies diplomas it was presented with and further processes the data inside.

# Lifecycle of a Diploma VC

1. Holder requests diploma from the issuer.
2. Issuer issues the diploma and (optionally) adds a proof of issuance of the diploma to the verifiable data registry.
3. Holder receives it and saves it to his mobile wallet.
  - Note: Credential storage is still uncertain. For privacy, a holder ideally only stores it on their device. Realistically, cloud wallet providers will be the popular choice.
  - Also note: A credential's holder is not necessarily also its subject (e.g., parent holding education credentials for child).
4. Holder presents VC (or VP) to the verifier.
  - Note: A verifier never directly receives VC from the Issuer.
5. Verifier checks signature(s) and also checks verifiable data registry for revocation status and proof of issuance of the diploma, if required.





- Verifiable Credentials take the form of a JSON (or JSON-LD) document and typically contain:
  - Context
  - Issuer
  - Issuance timestamp
  - Expiry timestamp (optional)
  - Type
  - Subject
  - Subject identity attributes
  - Cryptographic proof to ensure the integrity and authenticity of the VC

```
"@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://w3id.org/dcc/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
],
"type": [
  "VerifiableCredential",
  "DiplomaCredential",
  "ElmoDiplomaCredential"
],
"issuanceDate": "2022-07-04T08:54:48Z",
"issuer": {
  "name": "Technical University of Munich",
  "url": "https://www.tum.de",
  "image": "https://github.com/gopimehta/did-web-document/raw/main/resources/TUM_logo-440x236.png",
  "id": "did:web:dibiho.org:TUM.Test"
},
"credentialSubject": {
  "id": "did:web:dibiho.org:Lucas.Learner",
  "hasCredential": {
    "name": "B.Sc. Informatics",
    "description": "Awarded the academic title Bachelor of Science (B.Sc.) after completing the Informatics"
  }
},
"id": "http://localhost:8082/credentials/33",
"proof": {
  "type": "Ed25519Signature2020",
```

Start of an example credential for the digitalization of diplomas (DiBiHo Project).

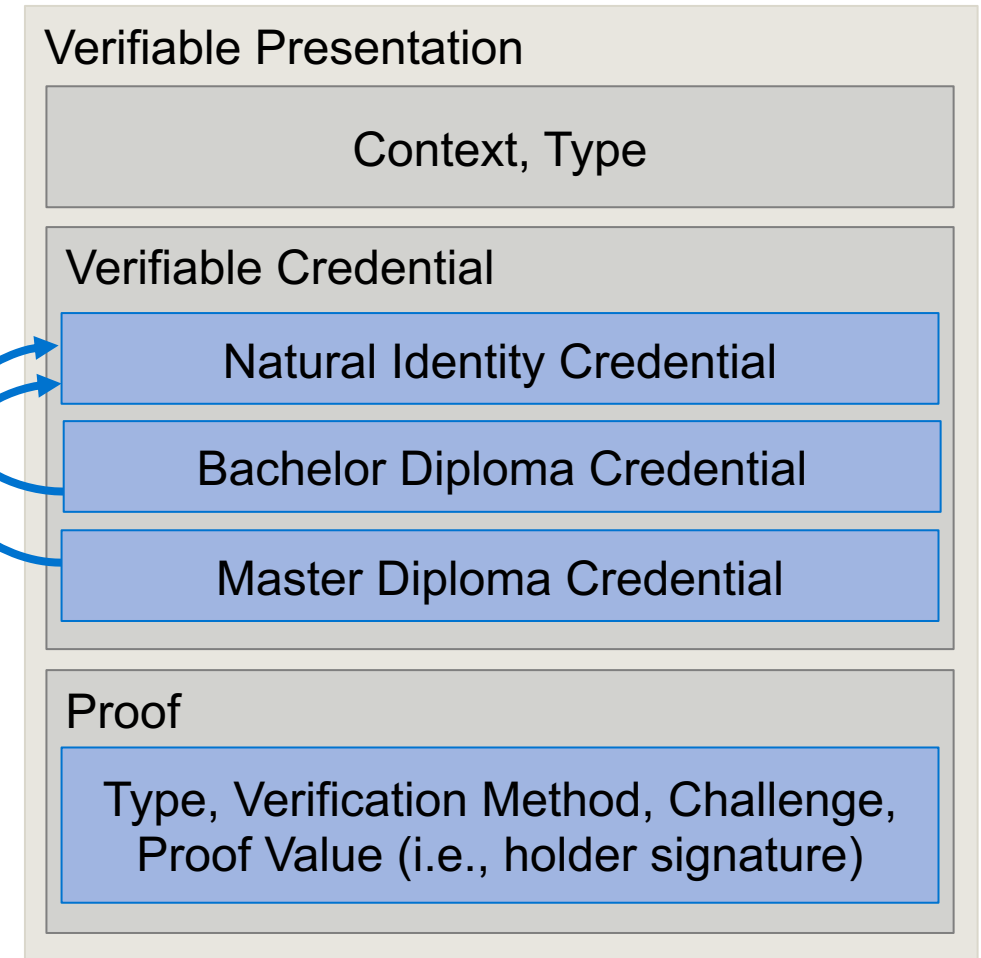
- **Verifiable Presentation:**

- A Verifiable Presentation (VP) is **data derived from one or more Verifiable Credentials** issued by one or more issuers that is specifically compiled for and shared with a specific verifier.
- Holders of VCs can generate VPs and then share these with verifiers to prove specific claims regarding their identity.

- **Selective disclosure:**

- Selective disclosure is a core concept of SSI, and it enables individuals to share no more of their private data than is strictly necessary for a given service.
- Issuers can issue VCs that support selective disclosure.
- If a VC supports selective disclosure, holders can create a VP containing only parts of the VC.

Hashlink



Slightly simplified example of a VP created by a university graduate presenting his degrees to a prospective employer.

## 1. Introduction

- Today's Digital Identity
- Problems with Today's Digital Identity
- Identity Paradigms
- Diploma Use Case

## 2. Self-Sovereign Identity

- Motivation
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers
- Protocols

## 3. SSI Use Cases

- Diploma Use Case
- Examples of SSI Usage

## 4. Challenges

- SSI Criticism
- Challenges

Google, Apple, and Mozilla filed official objections to the acceptance of the W3C DID 1.0 specification in September 2021. So, what was the reason for it?

Four main reasons were given:

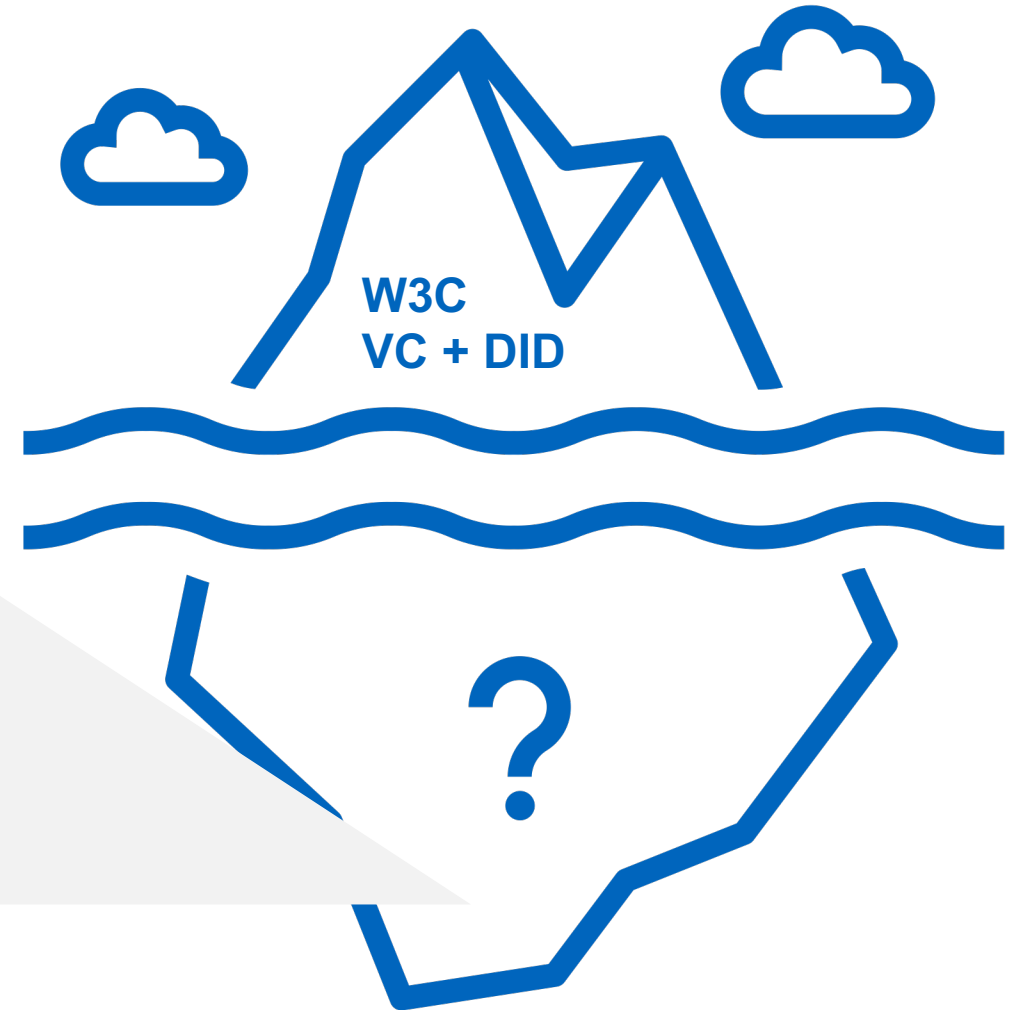
- The DID 1.0 specification standardizes DIDs in general but does not standardize any specific DID methods.
- The DID 1.0 specification encourages many different DID methods instead of just a few, which might limit interoperability.
- The DID 1.0 specification does not prohibit centralized DID methods.
- The DID 1.0 specification promotes the use of blockchains, about which environmental concerns have been raised.

But...

- Currently, there is no serious alternative to DIDs.
- Diversification means “plug and play,” ensuring interoperability and easier adoption for existing systems.
- Besides, all the objecting companies have a significant interest in staying a federated identity provider.

There was also some criticism of SSI in general from tech influencers who argue that most SSI use cases can be solved more easily using existing central authority database systems. While that is generally true, there are arguably benefits in researching and designing systems that do not needlessly centralize control and data. Technical criticism is rare.

- Many libraries are still in a very experimental state
- Many “VC-adjacent” functionalities have no viable standards
  - Status lists only have one standard that is arguably not sufficient: “Bitstring Status List v1.0”
- Wallet software is also still in its infancy
  - Usability is key and needs to be improved
- Loss of private keys is generally not recoverable
  - Backup solutions are simple if present at all
  - Should privacy be traded for usability (e.g., through cloud wallets)?
- The choice of DID methods is overwhelming, even for technical experts
  - Roughly 170 methods exist<sup>1</sup>
  - Very different characteristics spanning cost, features, and security
- General governance is hard and fundamental questions need solid answers that go beyond just technical contributions:
  - *If we encounter a diploma credential from an unknown university, how do we know if that issuer DID is actually a university?*
  - *And who is able/allowed/trusted to decide which issuers are trusted?*



<sup>1</sup>Hoops, F., Mühle, A., Matthes, F., & Meinel, C. (2023, July). A taxonomy of decentralized identifier methods for practitioners. In *2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)* (pp. 57-65). IEEE.



If you want to be actively involved in SSI research in some form, contact [Felix Hoops](#).

Some possible topics include:

- Quantifying the adoption of SSI
- Examining and solving governance challenges in SSI
- Contributing to smaller standardization proposals required to support VCs, such as status lists
- Establishing best practices in SSI
- ...