SSI & Decentralized Identity Management

Öz, B., Hoops, F., & Matthes, F. (2023). “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)
wwwmatthes.in.tum.de

Outline

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

2. SSI
- Motivation
- History and Phases
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers

3. SSI Use Cases
- Diploma Use Case
- Examples of SSI Usage

4. Challenges
- SSI Criticism
- Challenges

Digital Identity

- In the digital age, we need digital identity for offline and online services.

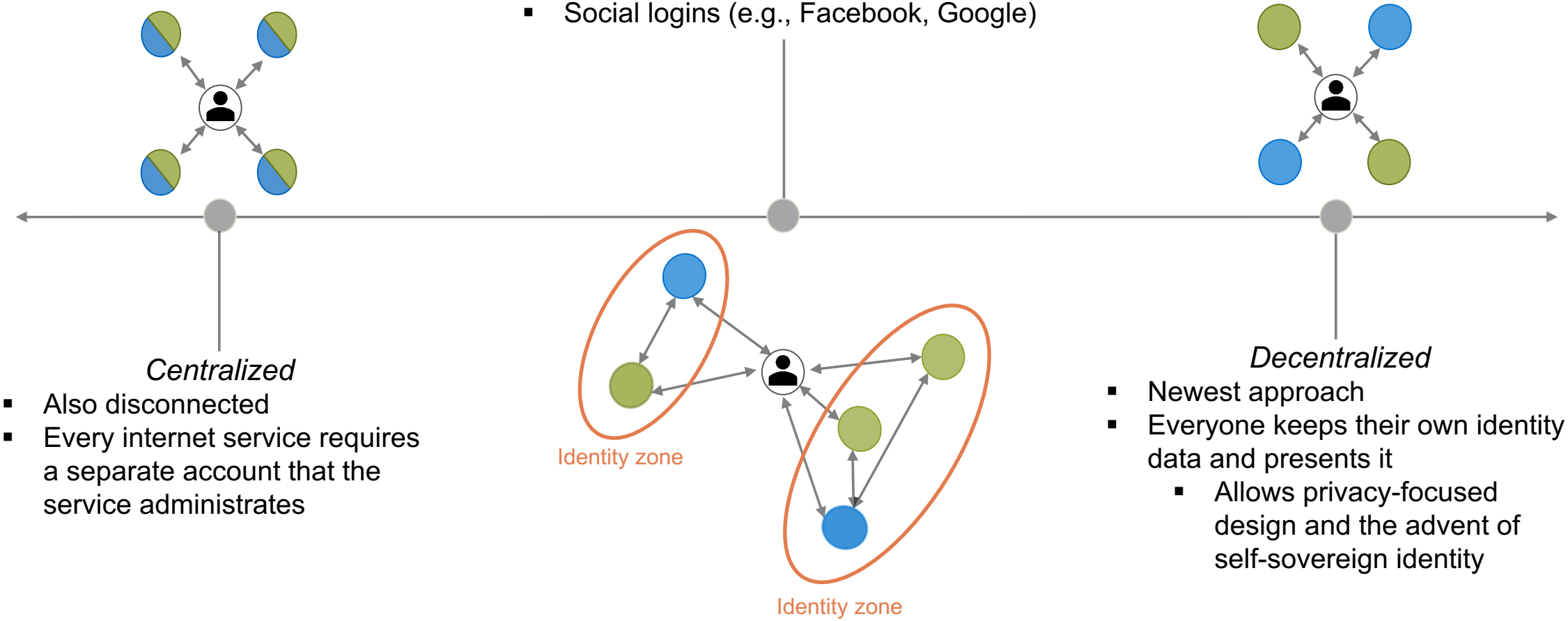
- Sometimes a pseudonymous identity, such as an email, is sufficient and other times we need our natural identity:
  - Social media accounts usually just require an email address
  - Banking requires natural identity verification for regulatory reasons

- 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.

Identity Paradigms



Problems with Today's Digital Identity

- 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 other countries, or even in their own.

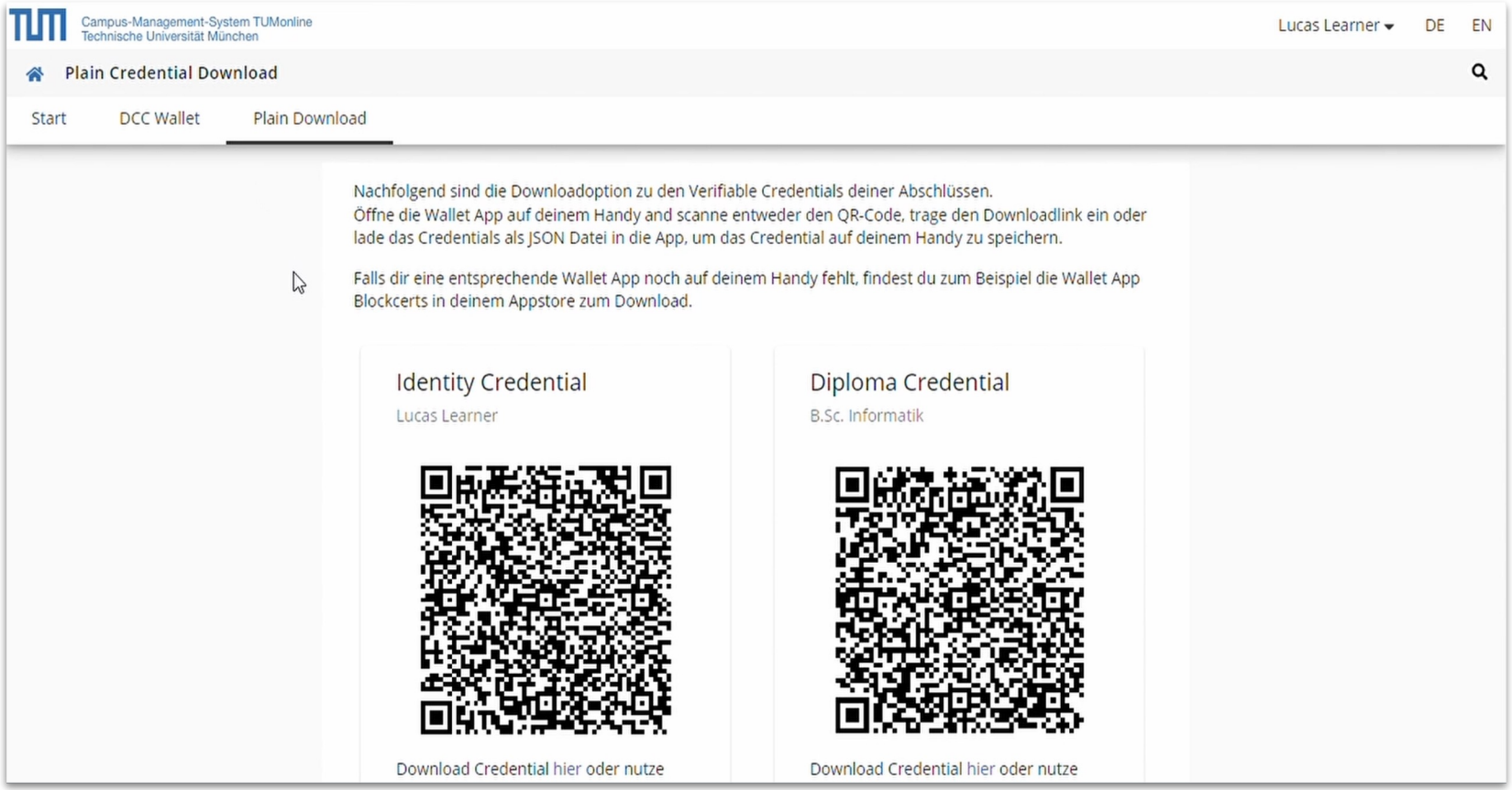
- Vendor Lock-in
  - Federated identity systems create vendor lock-in, limiting users choice and control.

- Big Identity Providers are Gatekeepers
  - Arbitrary account suspension
  - Censorship

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.

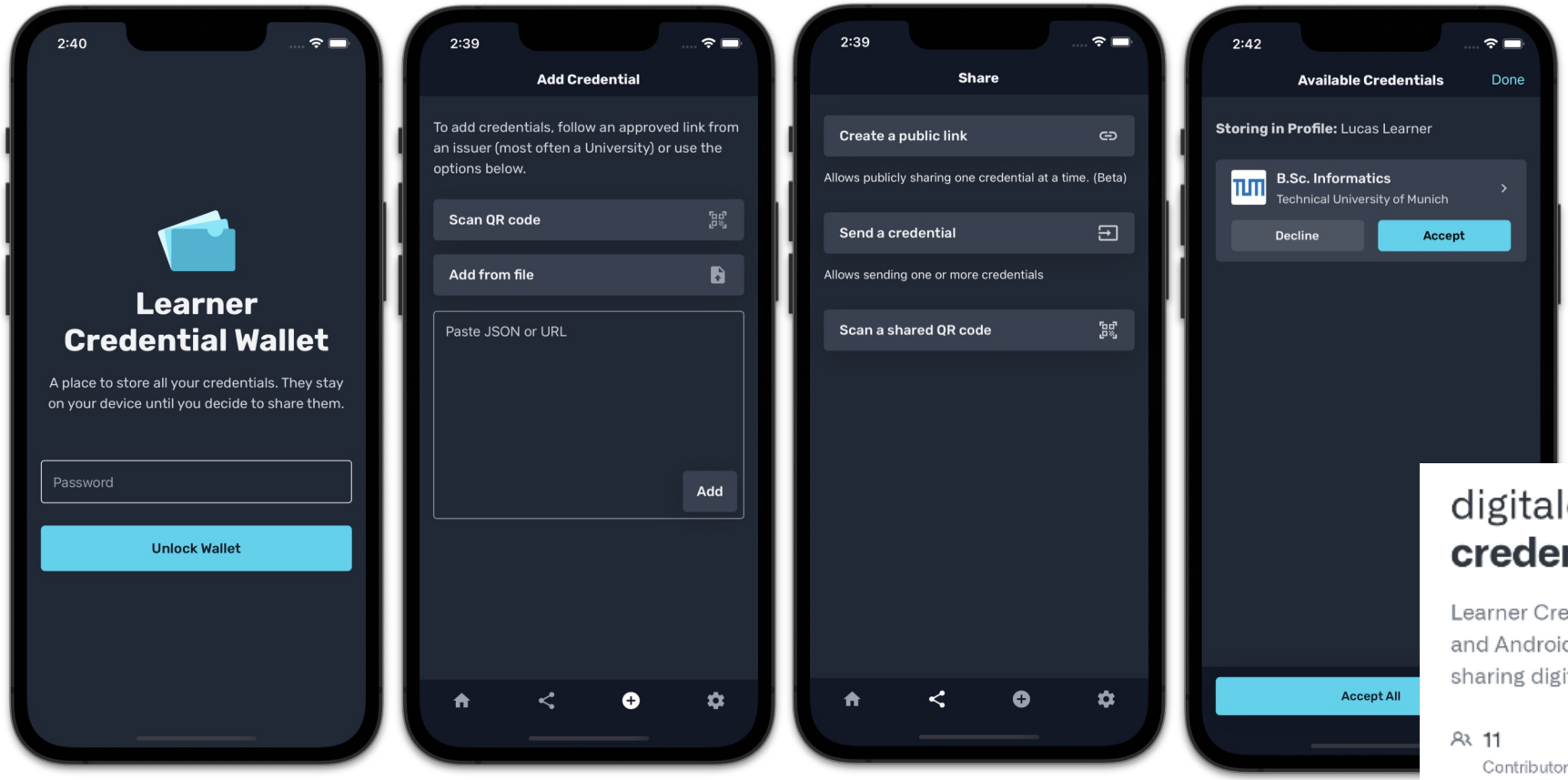
Use Case Preview: Diplomas

Students can receive a diploma credential from their university:

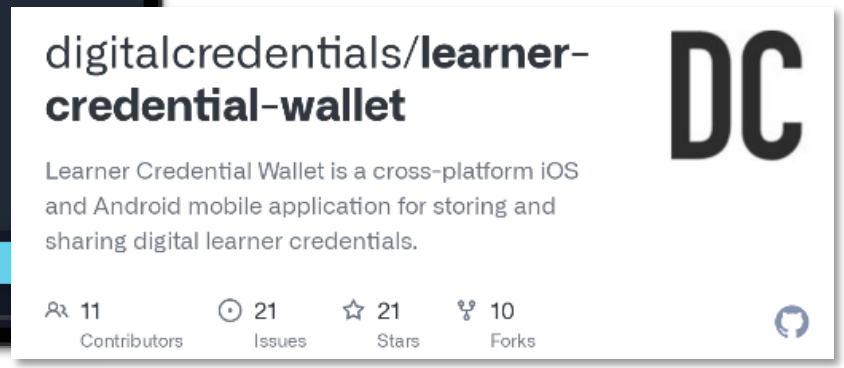


Use Case Preview: Diplomas (cont.)

Smartphone wallet apps are a convenient solution to always have your credentials with you:



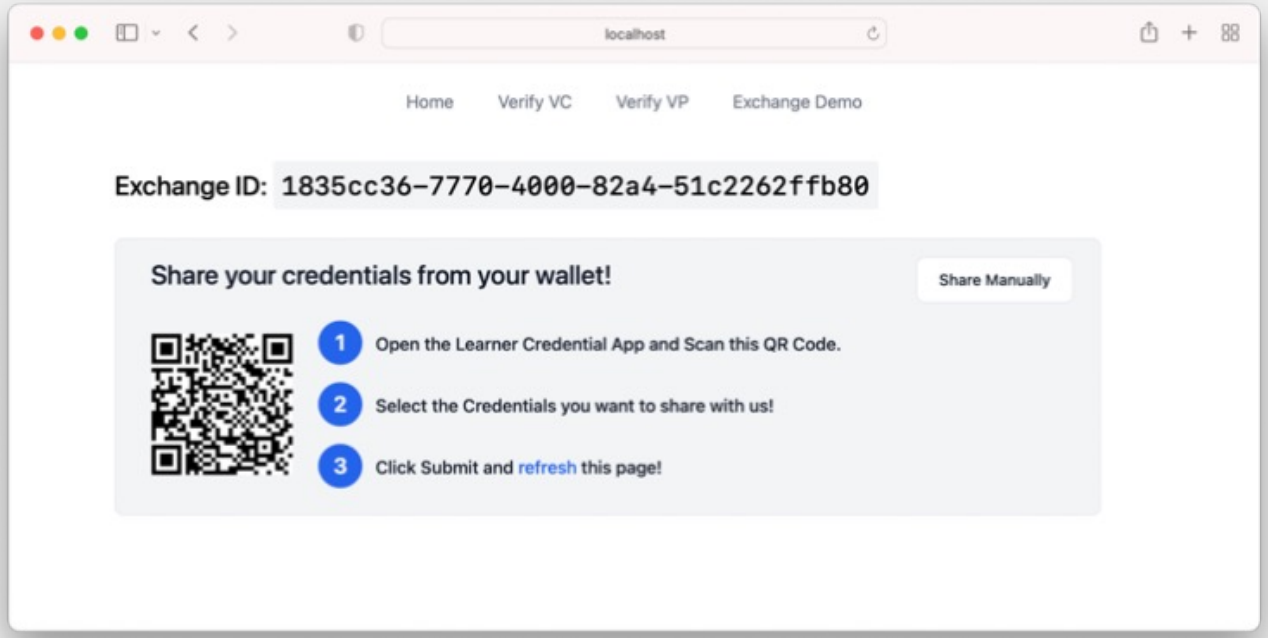
DCC DIGITAL CREDENTIALS CONSORTIUM



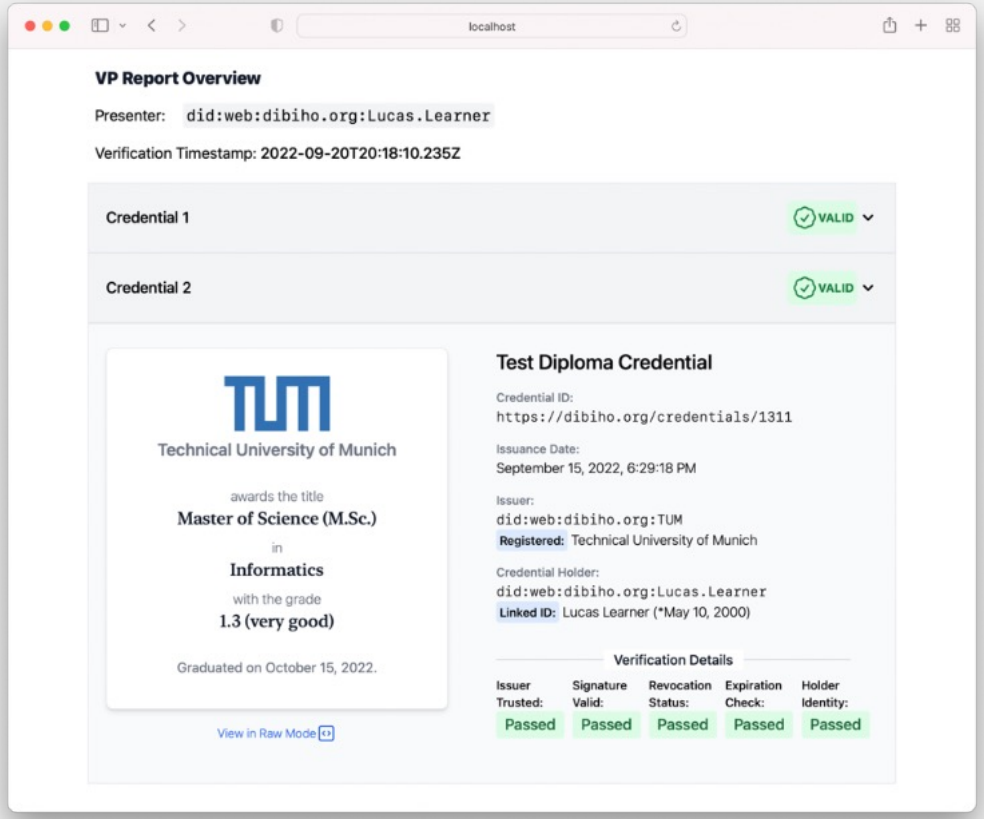
Use Case Preview: Diplomas (cont.)

Example of presenting/verifying a diploma credential to a third party

User View:



Relying Party View:



Outline

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

2. SSI
- Motivation
- History and Phases
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers

3. SSI Use Cases
- Diploma Use Case
- Examples of SSI Usage

4. Challenges
- SSI Criticism
- Challenges

The Motivation Behind SSI

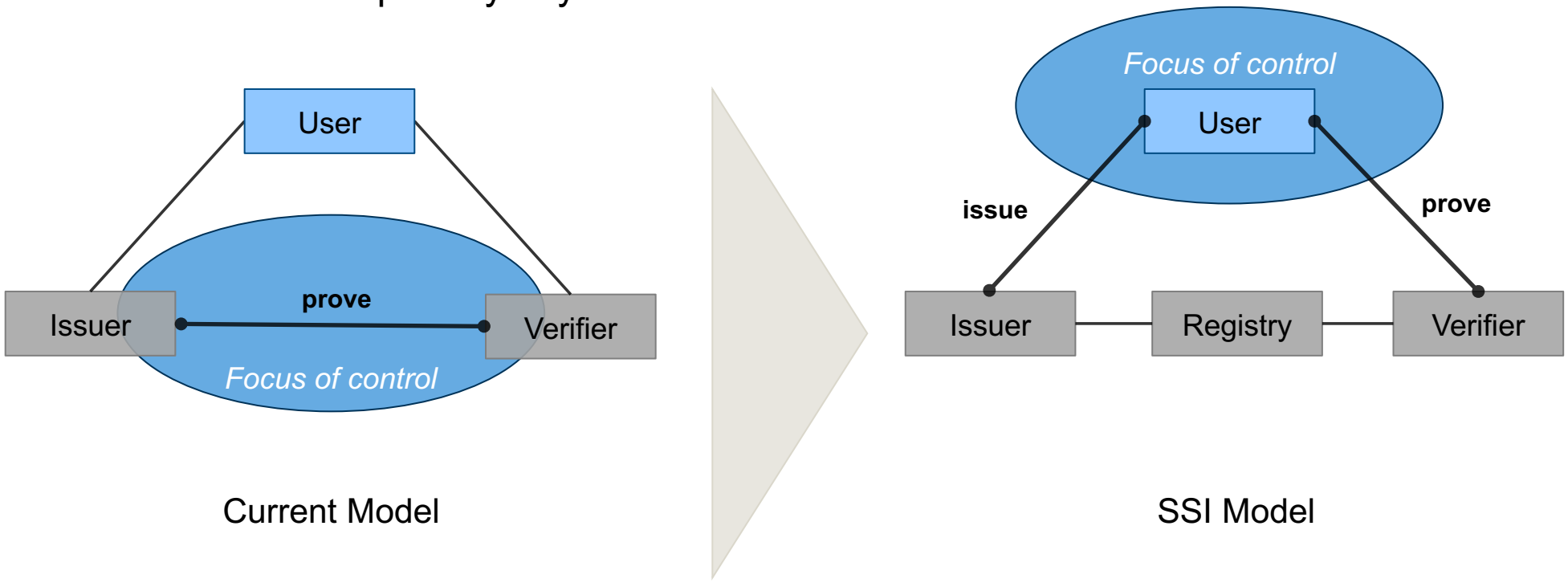
- Today's identity providers have immense amounts of power over us and metadata about us.

- Offline, we receive state-issued id cards, that we and only we 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 goal architecture.
- With SSI you can instantly create an account (i.e., identifier) without anyone being able to prevent that.
  - You alone control that account, which means no one can shut it down or take it over.
  - The account is accepted by any online service.



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

A Brief History of SSI

According to Christopher Allan, 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.

Another significant work that helped shape the idea of SSI was a paper by Carl Ellison in 1996, which argued for the need to establish identity without using certificates from trusted certification authorities.

Christopher Allen writes his influential blog post “The Path to Self-Sovereign Identity”[1]. This marks the beginning of increased activity towards realizing SSI.

In the following few years, some important W3C working groups are launched.

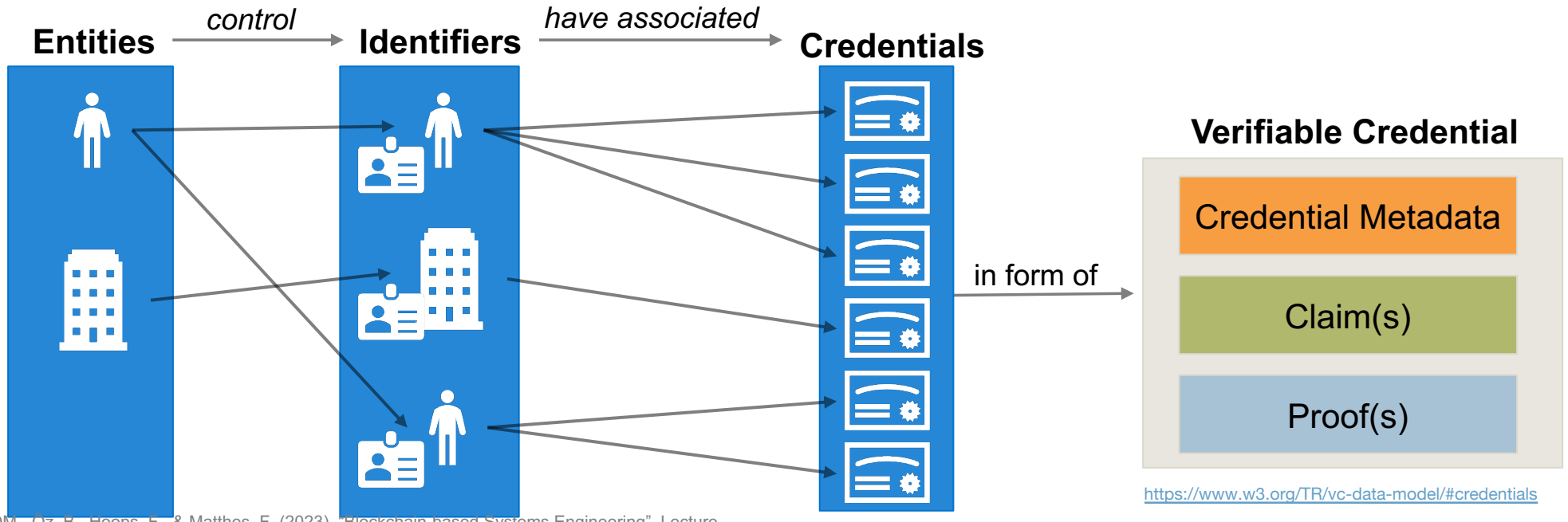
After W3C VC, W3C DID is finally becoming an official standard. With this, the core tools for SSI are standardized.

[1]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, thereby 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 school of design that puts privacy first. Entities can decide what attributes to present to whom.



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

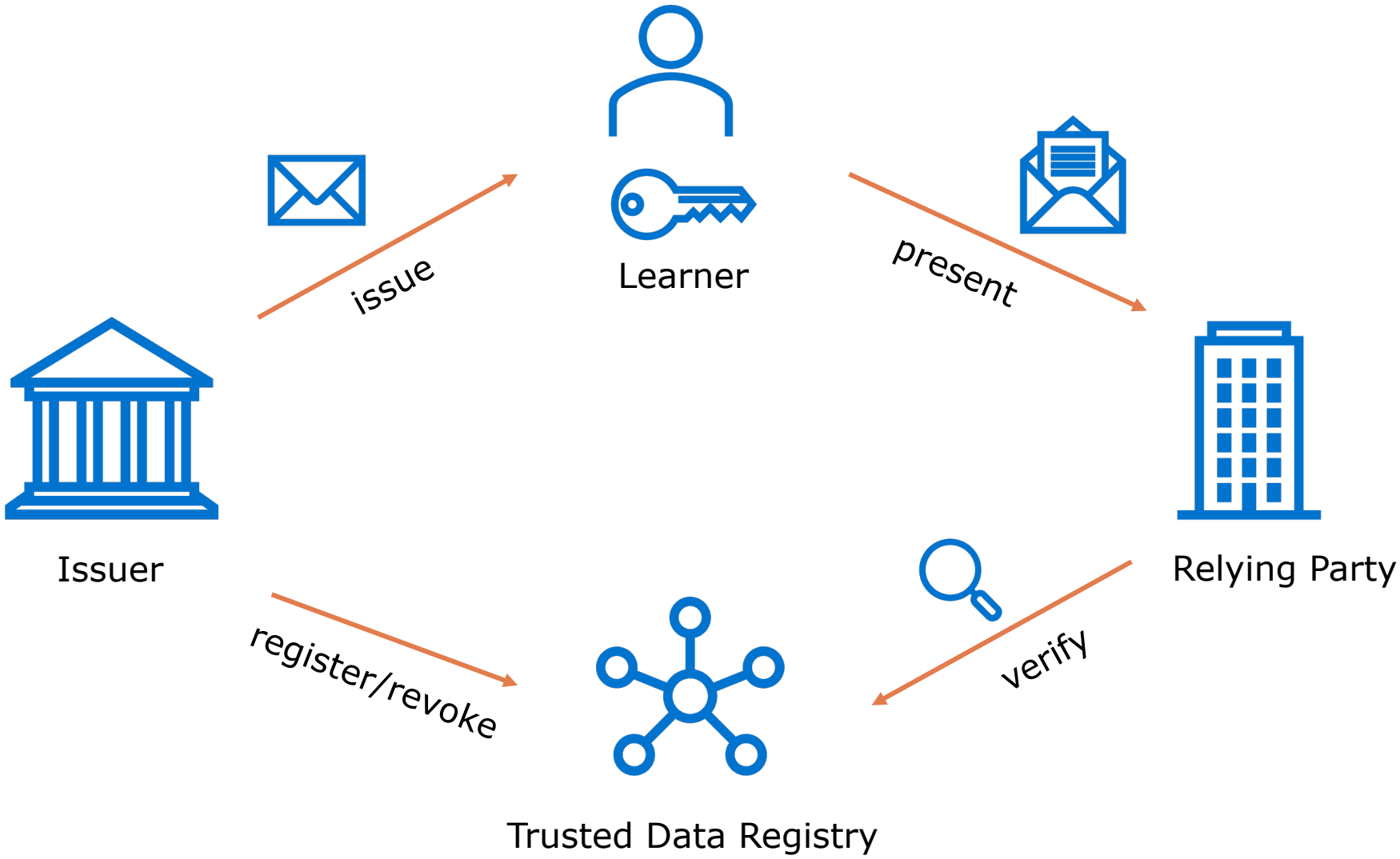
Principles of SSI[1]

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

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

[1]Christopher Allen's ten SSI identity principles.

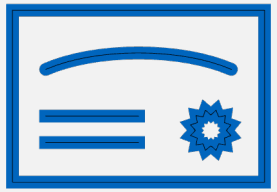
Lifecycle of a Verifiable Credential



10 SSI & Decentralized IDM - Öz, B., Hoops, F., & Matthes, F. (2023). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

SSI Technology

- 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.



Word Wide Web Consortium

Decentralized Identifiers

- Decentralized Identifiers (DIDs) are unique identifiers that are 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 a piece of software resolving 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, such as a blockchain.

DID Document:

- 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.

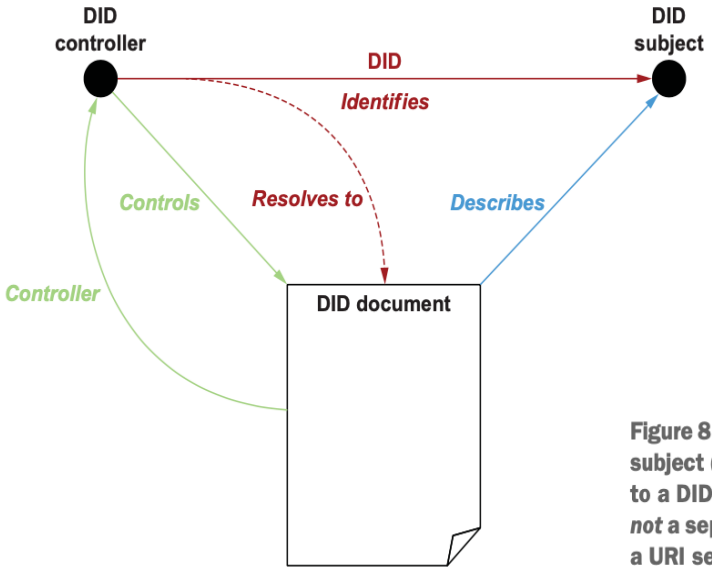


Figure 8.29 A DID always identifies a DID subject (whatever it may be) and resolves to a DID document. The DID document is *not* a separate resource and does *not* have a URI separate from the DID.

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.

https://www.w3.org/TR/did-core/

Decentralized Identifier Examples

They are very flexible due to their reliance on **custom DID methods**. A method mainly 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)

A DID is always represented by a string following the structure discussed in the examples below:

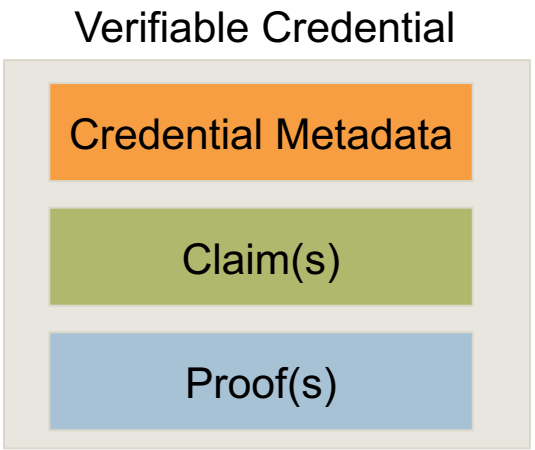
did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a		
Scheme This part is static.	**Method** Usually short and identifies one specific publicly documented DID method. This one provides high decentralization and low barrier of entry.	**Method-Specific Identifier** Arbitrarily long identifier. In this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

Verifiable Credentials

- **Verifiable Credential:**
  A Verifiable Credential (VC) is a digital representation of a set of claims that can be verified by a third party without the need for 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.

VC 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 certain claims regarding their identity.



Verifiable Data Registry

Unlike centralized identity systems, the identities of the users are stored in each user's wallet.[1] 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 used DID method.
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 even just one 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** makes 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)
  - Also provides consensus (e.g., on status lists)

[1]Similar to a physical wallet, an SSI digital wallet stores your Verifiable Credentials and your DIDs.

Outline

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

2. SSI
- Motivation
- History and Phases
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers

3. SSI Use Cases
- Diploma Use Case
- Examples of SSI Usage

4. Challenges
- SSI Criticism
- Challenges

Stakeholders for Digital Diplomas

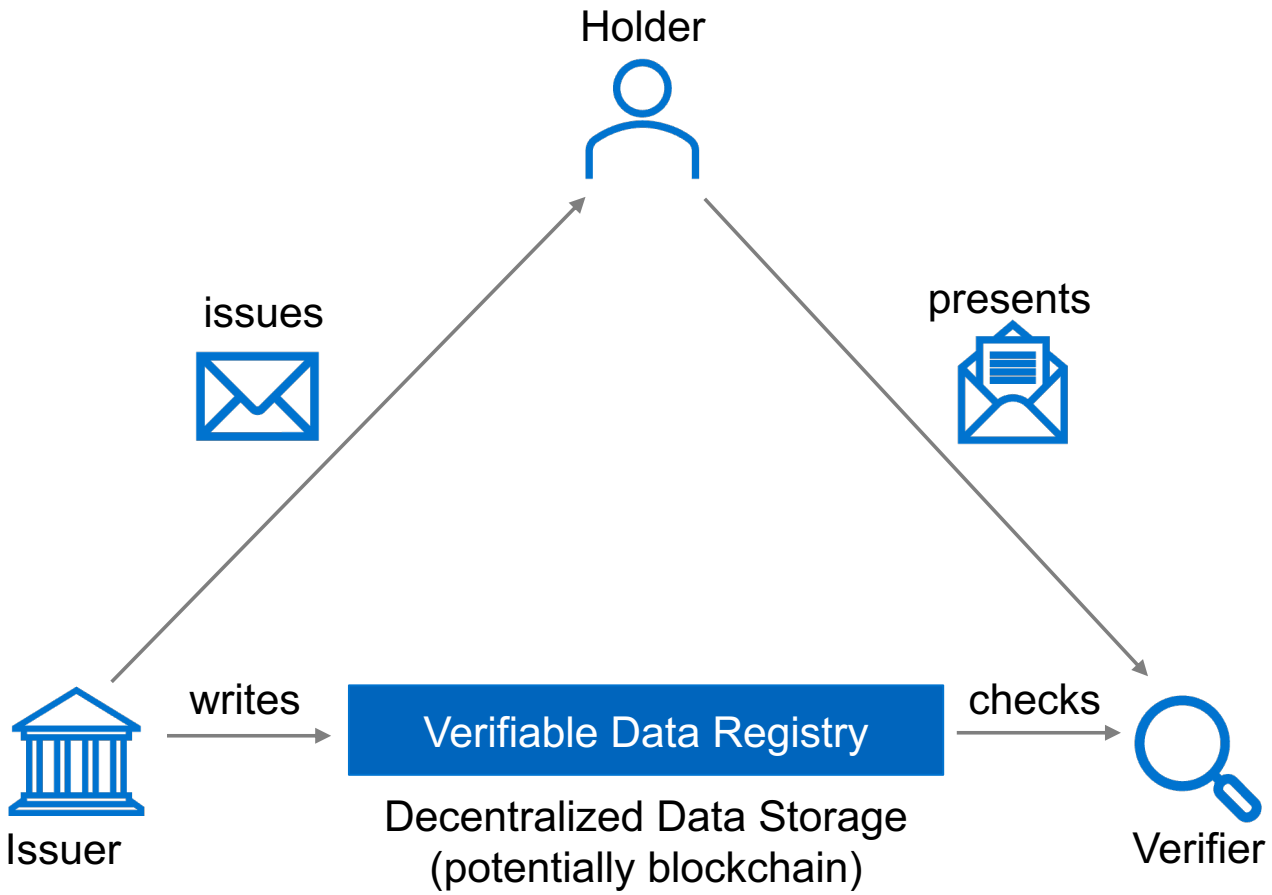
Universities issue digital diplomas in the form of VCs. This provides students with a convenient and secure way to access and share their academic achievements with other institutions, prospective employers, or anyone else they want to.

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.

10 SSI & Decentralized IDM - Öz, B., Hoops, F., & Matthes, F. (2023). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

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.



Diploma VC Structure

- 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

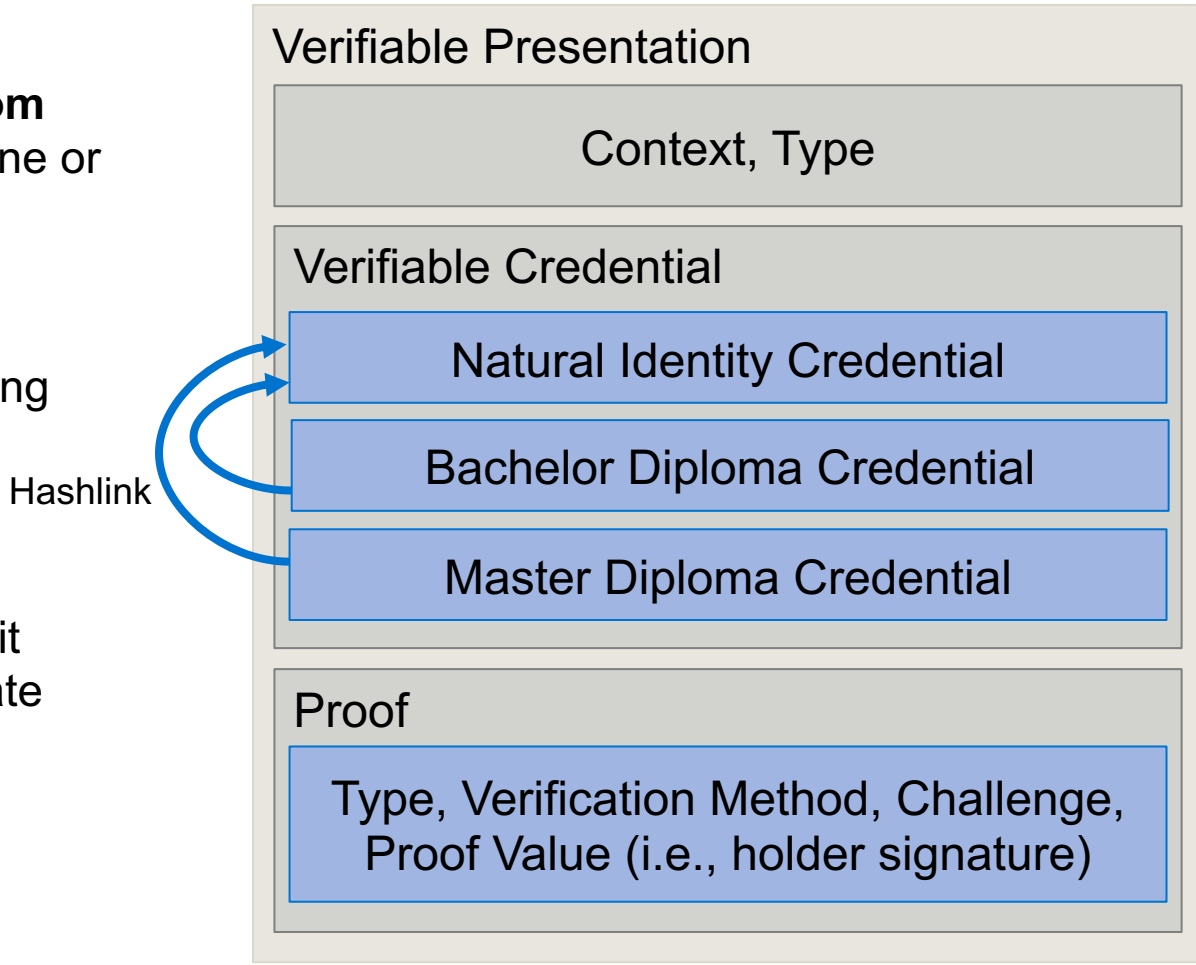

```
"@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://w3id.org/dcc/v1",
  "https://w3id.org/security/suites/ed25519-2020/v1"
],
"type": [
  "VerifiableCredential",
  "DiplomaCredential",
  "ElmoDiplomaCredential"
],
"issuanceDate": "2022-07-04T08:54:48Z",
"issuer": {
  "name": "Technical 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).

https://www.w3.org/TR/vc-data-model/

Diploma VP Structure

- **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 certain 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.



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

Early Examples of Production SSI Usage

The Digital Credentials Consortium was established in 2018 by 12 Universities, including MIT, Harvard, Berkeley and Technical University of Munich to develop “infrastructure for issuing, sharing, and verifying digital credentials of academic achievement”.

The Turkish Ministry of Foreign Affairs, in collaboration with the United Nations Development Programme, piloted Tykn’s[1] Self-Sovereign Identity solution to optimize the process of issuing Work Permits to refugees.

The government of Canada is using an open-source blockchain framework to streamline their services and cut red tape. Canadian companies claim they waste more than 6 billion Canadian dollars every year on unnecessary bureaucracy. This governmental project – The Verifiable Organizations Network – believes decentralized identities and trusted credentials are the solution.

GAIA-X aims to build a federated and secured data infrastructure for the European data economy based on the principles of openness, transparency and secure digital ecosystem. They have published a whitepaper which draws attention to the important role of the Self-Sovereign Identity (SSI) concept in the Gaia-X ecosystem.

[1]An award winning startup based in The Hague developing digital identity tools.
https://identityreview.com/on-the-horizon-tykn-and-social-impact-through-digital-identity/

Outline

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

2. SSI
- Motivation
- History and Phases
- Definition and Principles
- Verifiable Credentials
- Decentralized Identifiers

3. SSI Use Cases
- Diploma Use Case
- Examples of SSI Usage

4. Challenges
- SSI Criticism
- Challenges

SSI Criticism

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.

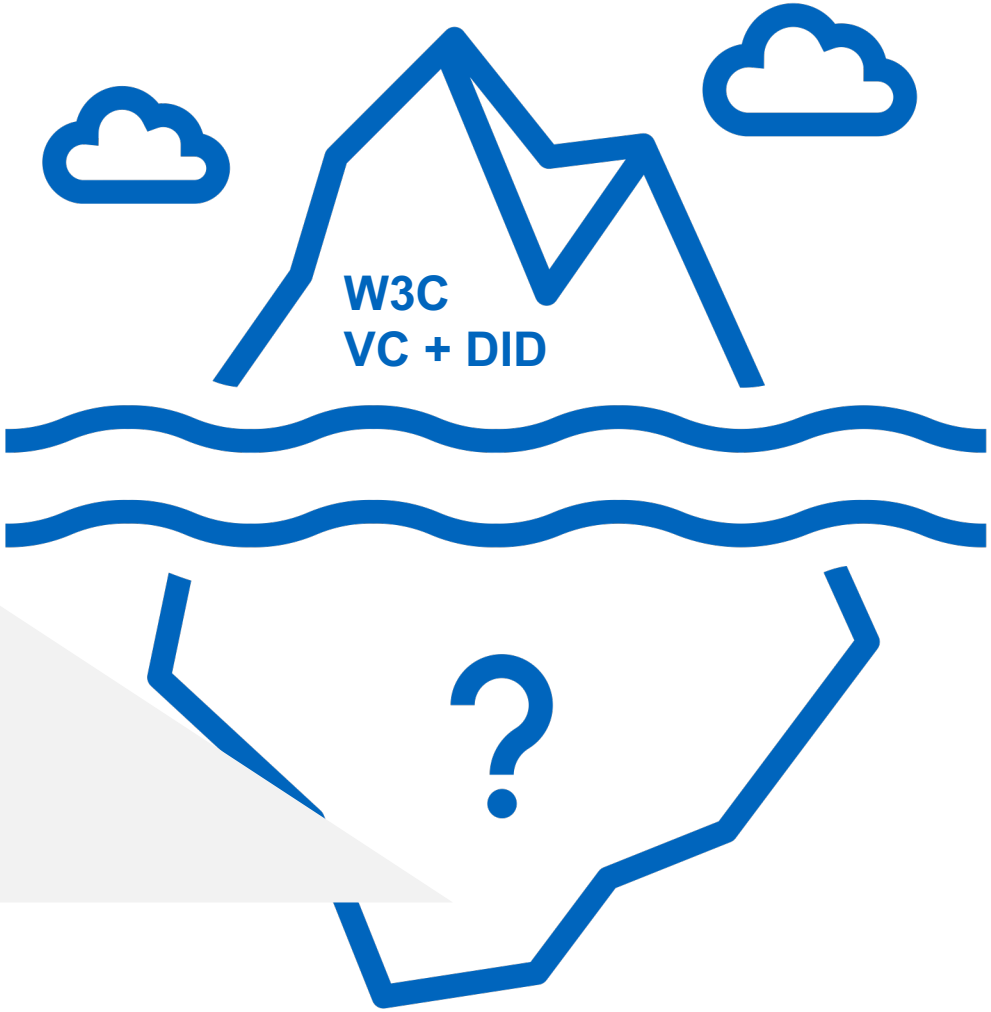
But…

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

There was also some criticism on SSI in general coming from tech influencers who argue that most SSI use cases can be solved easier 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.

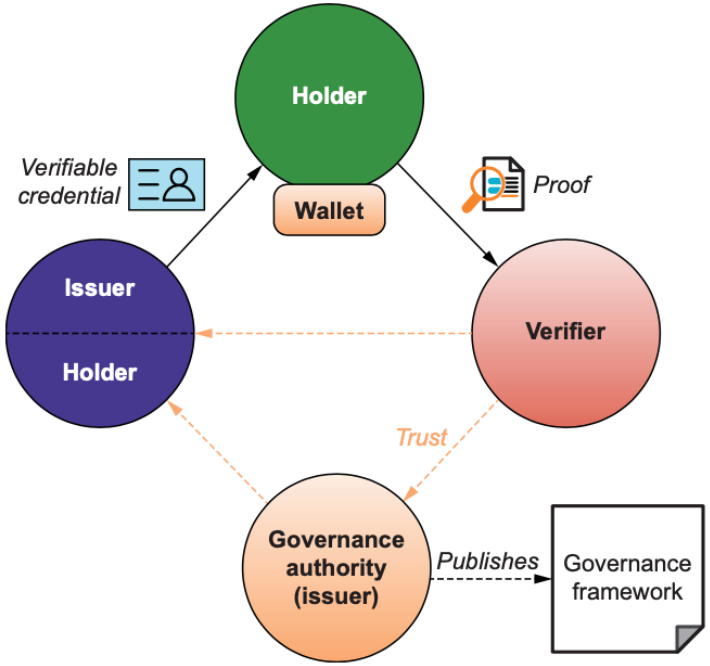
Implementation Challenges

- 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: StatusList2021
- 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
  - Very different characteristics spanning cost, features, and security



Governance Challenges

- Governance is one of the major challenges in SSI.
- Consider an example:
  - *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?*
- Similar problems arise for other types of credentials with real world impact.
- A “Trusted Issuer Registry” is often stated as a solution to decide **which issuers are trusted**. Good implementations of this are similarly **unsolved** like revocation.
  - For example, on a national level, a country’s ministry of education could provide a list of universities.
  - However, government involvement might not be desirable in all cases. Also, it might prove very difficult to find a single institution that has the trust of all participants world-wide.



Basic trust triangle for Verifiable Credentials (top half of figure) and the governance trust triangle (bottom half of figure).

Get Involved

If you want to be actively involved in SSI research in any 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
- Creating and improving the SSI user experience
- …