Micro Lecture - Self-Sovereign Identity

Öz, B., Hoops, F., & Matthes, F. (2022). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

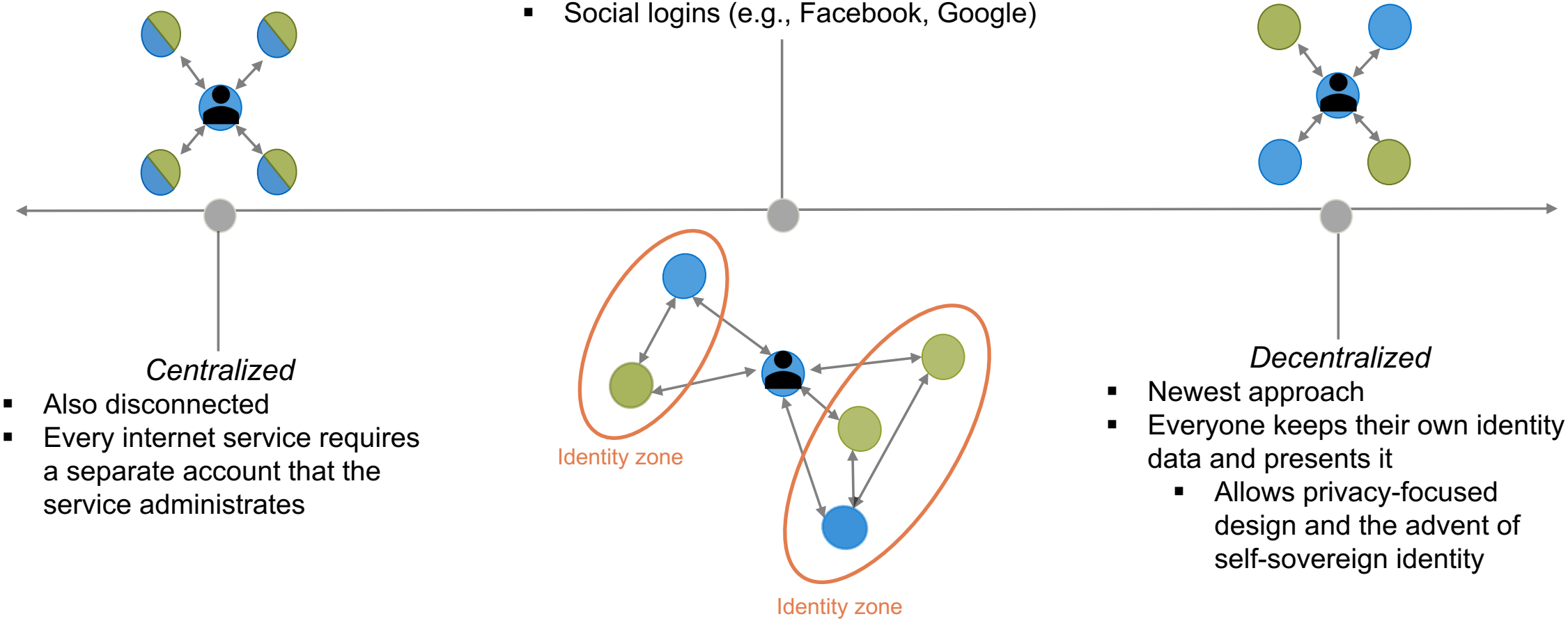
Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. Decentralizing Identity Management
   - Identity Paradigms
   - Motivation & Use Case Example

2. Self-Sovereign Identity
   - Definition
   - Verifiable Credentials
   - Decentralized Identifiers
   - Governance Challenges
   - SSI Criticism

Identity Paradigms



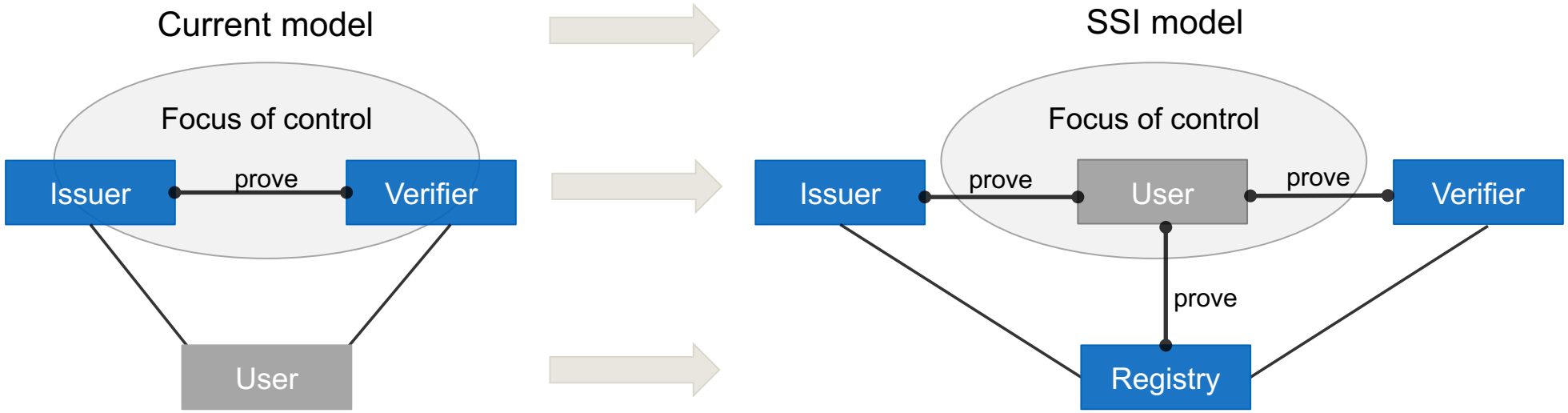
The Motivation behind Decentralized Identity

- 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 Decentralized Identity (cont.)

- Self-Sovereign Identity (SSI) is the term used to describe this goal architecture.
- With SSI you can instantly create an account (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.

Digital Diploma Use Case

Issuer, holder and verifier together form a ”trust triangle”

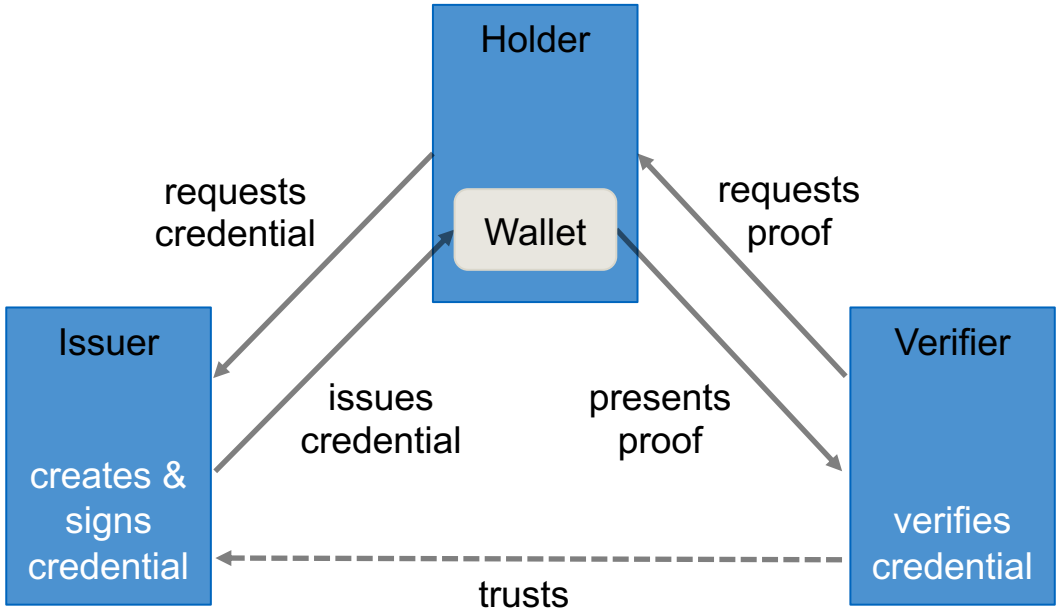
Holder:
- Requests *Verifiable Credentials*[1](VC) from issuers, keeps them in a wallet and presents them when requested.
- Could be a university alumnus that wants to apply to a company for a job.

Issuer:
- Issuers are the source of VCs
- Could be a university issuing a diploma to a graduate

Verifier:
- Relies on claims in VCs
  - Signatures allow verification
- Could be a company verifying an applicant’s university diploma

What hardware/software will be used in this experience?

- Most likely similar to today’s digital boarding passes or event tickets
- Holder probably uses a mobile wallet app
- Issuer and Verifier probably have a website that holder can interact with (directly on phone or via scanning QR code from another device)



[1]A set of information that some authority claims to be true about you, which is automatically verifiable. Deeper explanation on upcoming slides.

Outline

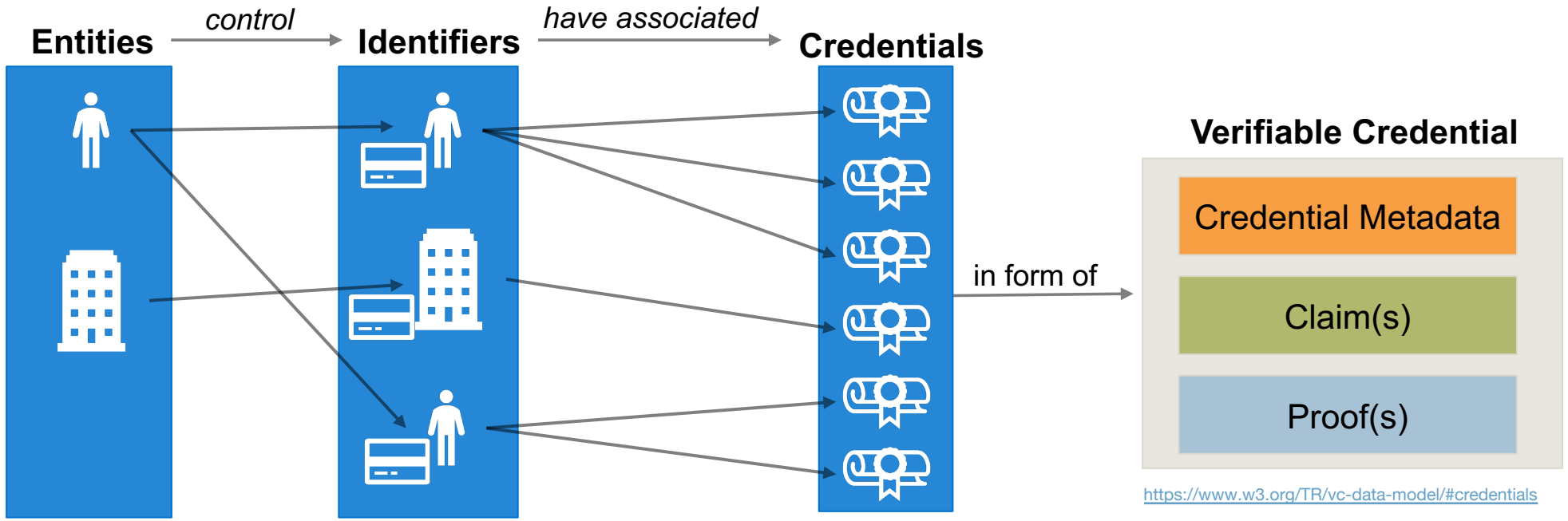
1. From Blockchain to SSI
- Identity Paradigms
- Motivation & Use Case Example

2. Self-Sovereign Identity
- Definition
- Verifiable Credentials
- Decentralized Identifiers
- Governance Challenges
- SSI Criticism

Definition

- Self-sovereign identity (SSI) is still a very new approach, thereby definitions vary slightly.

- General/Core 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

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) : DID, an identifier for every entity in the SSI ecosystem, is the first essential notion (and W3C standard draft[1]) under the SSI paradigm. A DID, in particular, is a globally unique identification that does not need the use of a centralized authority. An example of a DID is *did:example:123456abcdef*.
  - **Verifiable Credentials** (VC): VCs are 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.

[1]DID is still not officially a standard yet, it is just a draft.

Verifiable Credentials

- Verifiable Credentials take the form of a JSON (or JSON-LD) document and typically contain:
  - Context
  - Issuer
  - Issuance timestamp
  - Expiry timestamp
  - 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",
```

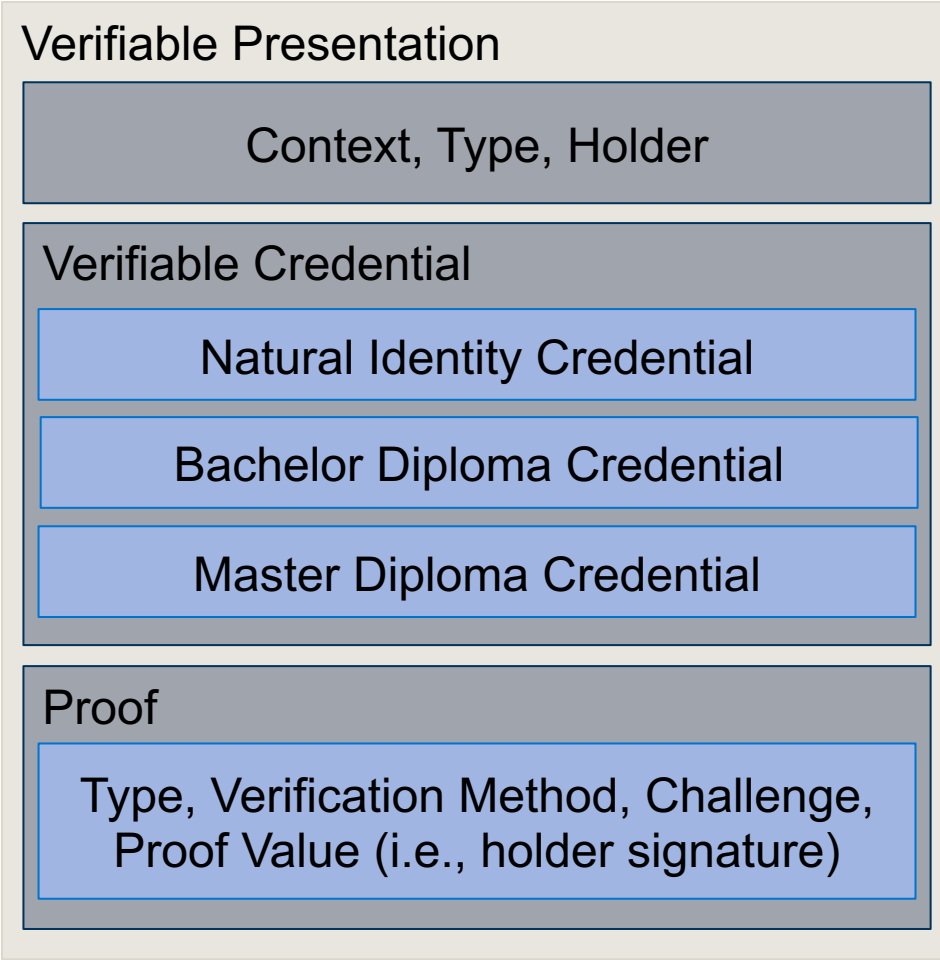

Start of an example credential for the digitalization of diplomas (DiBiHo Project).

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

Verifiable Credentials (cont.)

- **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.

Verifiable Data Registry

- Unlike centralized identity systems, the actual identities of the customer/users are stored in the customer'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 functionalities:

1. **Logging**
   - Optional, but provides auditability (e.g, to detect fraudulent activity).
2. **Revocation**
   - Required, as there are many reasons to revoke a previously issued credential.
   - There is still no good, universally accepted solution for revocation.

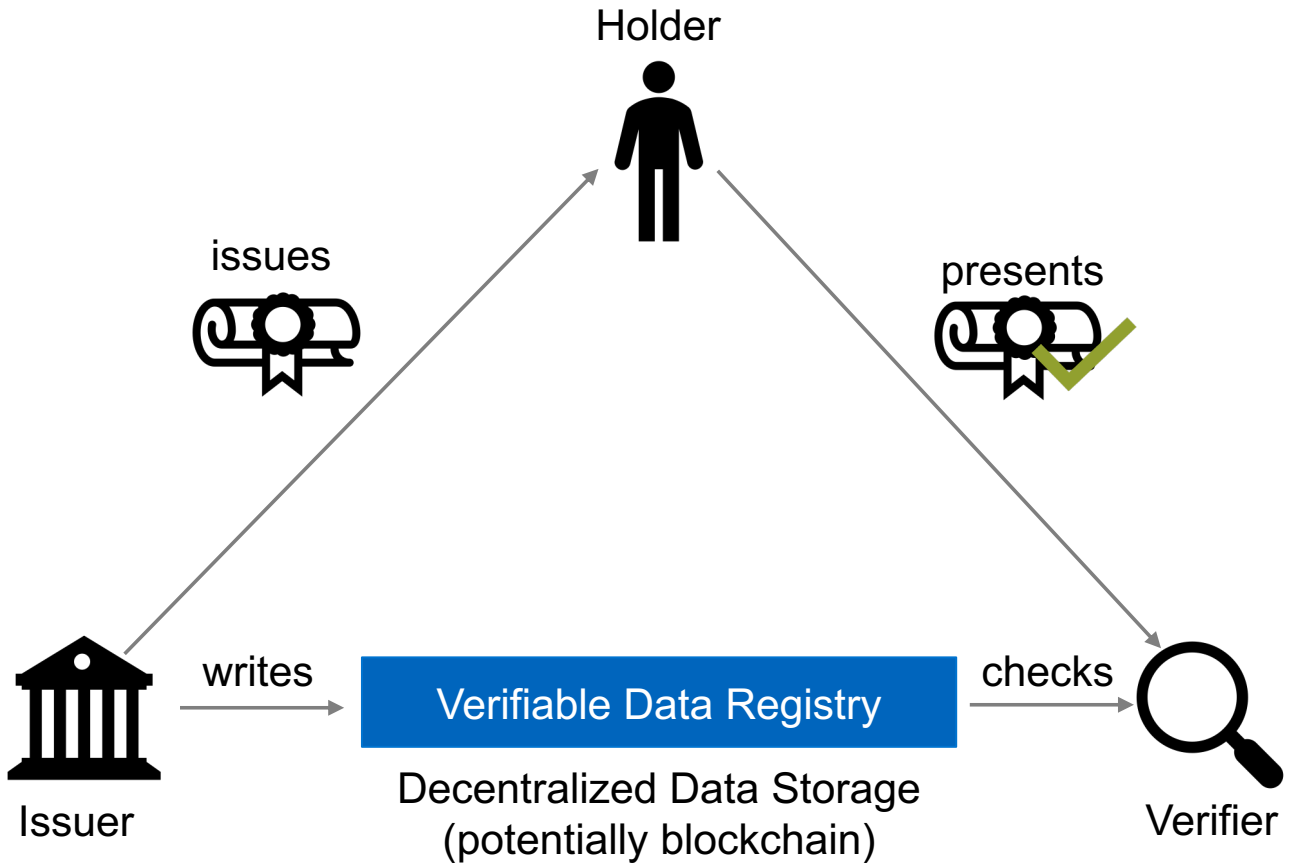
The publicly readable Verifiable Data Registry should never expose private information (e.g., credentials themselves). **Data stored there is typically minimal, such as serial numbers or hashes of credentials.** Exact data and data structure are implementation-specific.

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 (on revocation and issuance logs)

[1]Just like a physical wallet, an SSI digital wallet stores your Verifiable Credentials and your DID.

Lifecycle of a Verifiable Credential

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.



Decentralized Identifiers

VC can theoretically work with many different types of identity, however DIDs are the preferred solution. 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** 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	**Method**	**Method-Specific Identifier**
This part is static.	Usually short and identifies one specific publicly documented DID method. This one provides high decentralization and low barrier of entry.	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	**Method**	**Method-Specific Identifier**
This part is static.	Usually short and identifies one specific publicly documented DID method. This one enables easy adoption for institutions via an existing web presence.	Arbitrarily long identifier. In this case, it is a domain hosting a DID document at default relative path “/.well-known/did.json”.

Decentralized Identifiers (cont.)

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.

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.

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.

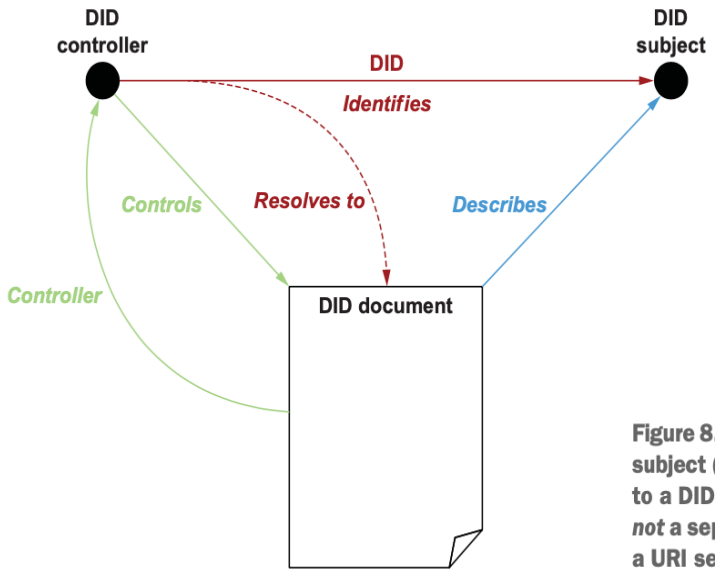
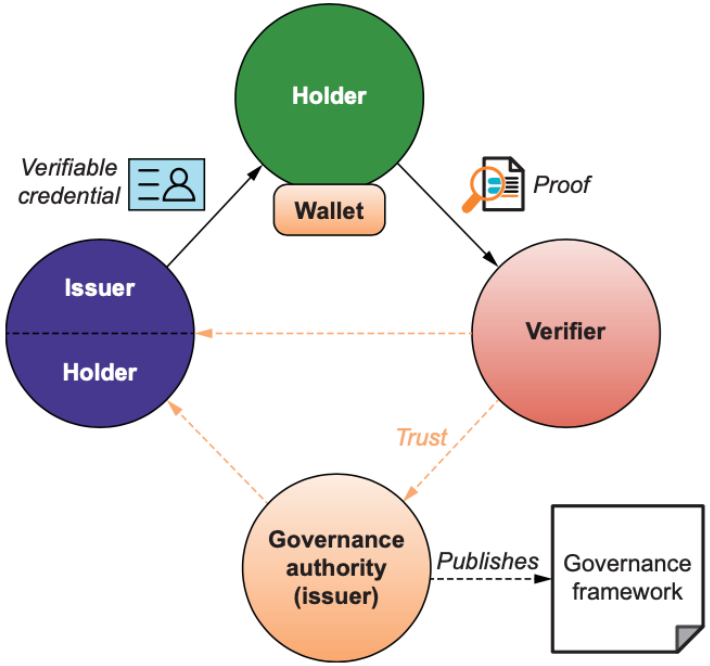


Figure 8.29 A DID always identifies a DID subject (whatever it may be) and resolves to a DID document. The DID document is *not* a separate resource and does *not* have a URI separate from the DID.

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

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).

Self-Sovereign Identity Decentralized Digital Identity and Verifiable Credentials- Alex Preukschat, Drummond Reed

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 is 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.

Early Examples of SSI Usage

The Digital Credentials Consortium was created 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, is piloting 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.

[1]An award winning startup based in The Hague developing digital identity tools.
https://tykn.tech/verifiable-credentials/#Privacy_and_Verifiable_Credentials

How You Can 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
- Establishing best practices in SSI
- Creating and improving the SSI user experience
- …