openHPI Course: Blockchain – Revealing the Myth

Blockchain Application Areas: Identity Management

Prof. Dr. Christoph Meinel
Tatiana Gayvoronskaya
Hasso Plattner Institute
University of Potsdam, Germany

Digital Identities

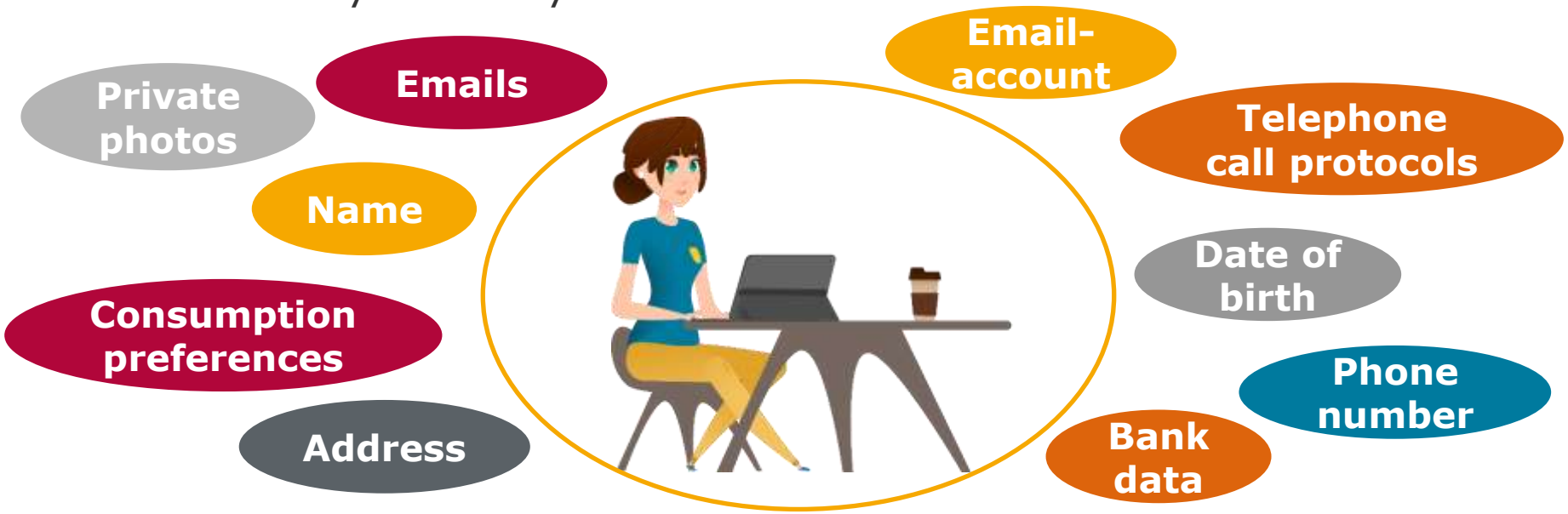
Identity management independent from any third party has been a desired goal of most users of digital services for years

- **How many accounts / digital identities** you already have for your digital services?
  - average user has **26+ digital identities** …
- **Objects** are also **linked to digital identities**, e.g., **IoT** devices (to **clearly assign tasks to these devices)**

Sharing of Personal Data

Every **digital identity** is constituted by **various sensible data** that **reveals information** about the person or object behind it

- Often they are simply **secured with a single password** and the **trust in the service provider**
- And we are **struggling** with the **flood of passwords** that are necessary for every service …



Partial Authorization for Certain Data

From the **user perspective** it would be desirable to give the **different online services only a partial authorization** for certain of these identity data

- So-called **self-sovereign identities** (**SSI**) allow the user to
  - remain in control of his own data
  - decide who is allowed to access which of the personal data and for how long

Self-Sovereign Identity (SSI)

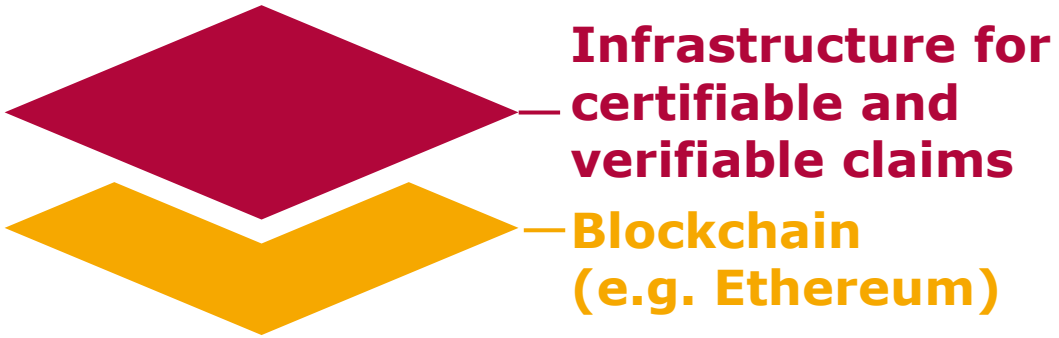
To this end, a **decentralised trust infrastructure** needs to be established

- We already know, that **blockchain technology** would be a **good candidate.** However, here is only one problem:
  - **personal identity data** as, e.g., **driving licence** would perhaps **not be checked** when **opening a bank account**, but in case of a **traffic control** they **should be verifiable**
  - so it is **not enough**, that the **data** and **its execution** in the system **cannot be manipulated**
  - we need a **confirmation** from a **trustworthy third** party that the **data** stored in the system **are true**

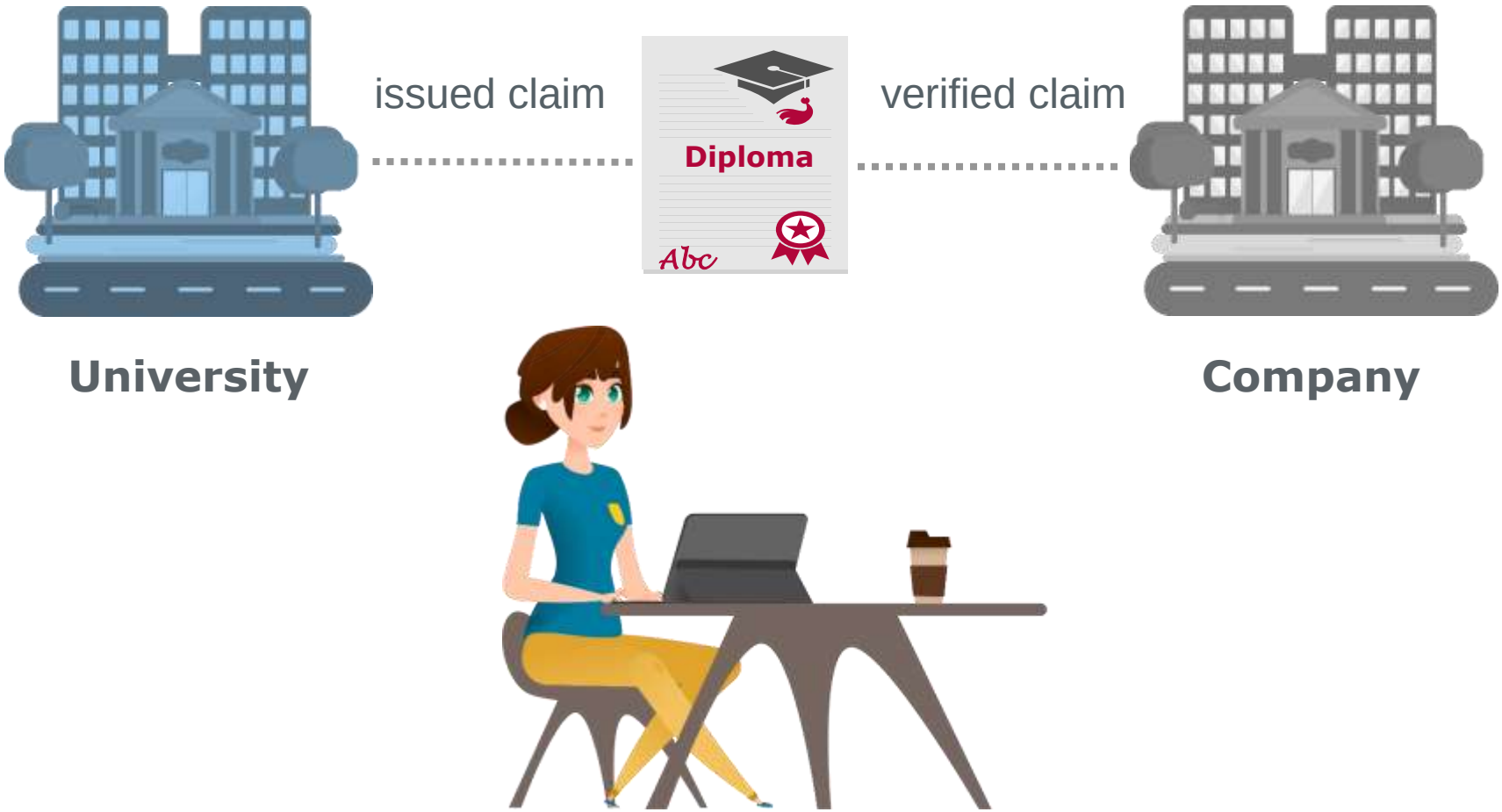
Claims – Statements About Identities

This means, **we need an infrastructure,** that **enables** us to make **statements about our identity**, so-called **claims**, that can be **certified** and **verified**

- Such statements can represent
  - address
  - ownership of a valid driver's license
  - credit standing
  - membership in a chess club
  - degree certificate
  - retirement, etc.



Example for Self-Sovereign Identities – Applying for a Job



Implementation Standards for Self-Sovereign Identities

World Wide Web Consortium (**W3C**) has proposed foundations for **SSI**s which have become standards:

- "**Verifiable credentials**" and
- **Decentralized Identifier**, or **DID** for short

Verifiable Credentials Ecosystem

- **Verifiable credentials** are the previously mentioned **claims**
- **Issuer** (university) and **subject** (learner) have their **own unique identifiers** (DID)
- **DID's** ensure that the **verifiable credential** has been issued **by a real issuer** and **has not been tampered with**
- **Individuals** and **organizations** can generate **their own identifiers**, as many as necessary

Issuer

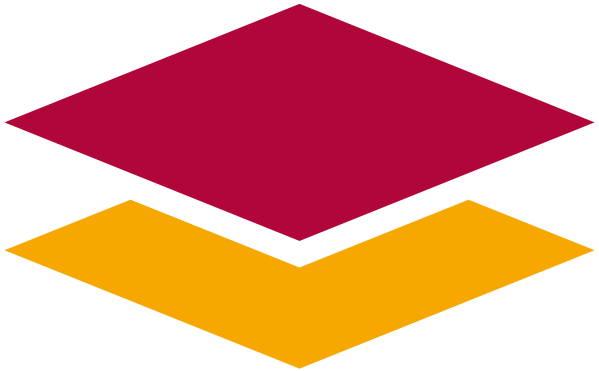
did:education:123456789abcdefghijk

Subject

Verifier

Verifiable Credentials Ecosystem Benefits

- **SSI concept** with **DIDs** and **verifiable credentials** is **based on a decentralized infrastructure** and makes a **central registries obsolete**
- There are numerous **SSI projects** which are using **public** or **private blockchains**
- Others see **more potential** for a **self-sovereign identity** in the so-called **Distributed Ledger Technology** (DLT)



Summary

- **Self-sovereign identities** (SSI) allow users to **remain in control** of **their identity data**
- **SSI**s **require** the establishment of a **decentralized trust infrastructure**, which allows the user to make claims about their identity
- The **best-known foundation** for such an infrastructure is the **Verifiable Credentials ecosystem** from W3C
- It offers **open standards** for so-called **DIDs** and **verifiable credentials**
- Numerous **SSI projects** use **public** or **private blockchains**
- Others see **more potential** in **Distributed Ledger Technology**

Recommended Literature and References

Recommended literature:

For a **broad overview** on subject of **Verifiable Credentials ecosystem**, we would recommend the following descriptions made by W3C

- **Verifiable Credentials Data Model 1.0**
- **Decentralized Identifiers (DIDs) v1.0**