Pre-Class Discovery: Self-Sovereign Identity

Digital Finance – BSc Course — Prof. Dr. Joerg Osterrieder

Complete before class. No prior knowledge required. Work alone or in pairs.

Activity 1: The Privacy Audit

Take out your passport (or imagine it). It contains: full name, date of birth, place of birth, nationality, photo, signature, passport number, address, and machine-readable zone data.

(a) You want to prove you are over 18 to enter a bar. List every piece of information your passport reveals *beyond* your age when you show it to the bouncer.

(b) Design a system that lets you prove "I am over 18" without revealing *any* of those other fields. Describe it in 3–4 sentences.
Hint: think about who could issue a yes/no credential.

(c) What technology concept allows proving a statement is true without revealing the underlying data? (You may guess—we will cover this in class.)

Activity 2: The Trust Triangle

Self-sovereign identity uses three roles: **Issuer**, **Holder**, and **Verifier**.

(a) For a **university degree**, identify who plays each role:

Role	Who?
Issuer	
Holder	
Verifier	

(b) Draw the trust triangle: how does the Verifier confirm the credential is genuine without contacting the Issuer directly?

(c) What role does a blockchain play in this model? (It does *not* store your personal data.)

Activity 3: Key Management Nightmare

You lose your phone. Your entire digital identity wallet is on it.

(a) Design 3 different recovery mechanisms. For each, describe the method in one sentence and identify the tradeoff between convenience and security.

#	Recovery method	Tradeoff
1		
2		
3		

(b) Which mechanism would you personally choose? Why?