Pre-Class Discovery: Self-Sovereign Identity — SOLUTIONS

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?

Answer Key

A1: (a) Full name, exact birth date, birth city, nationality, passport number, photo, signature, address—far more than needed. (b) A government issues a "verifiable credential" containing only the claim "age $\geq$ 18," signed cryptographically. The holder presents only this credential; the verifier checks the signature without seeing the passport. (c) Zero-knowledge proof (ZKP).

A2: (a) Issuer: university. Holder: the graduate. Verifier: an employer or another university. (b) Triangle: Issuer signs credential $\rightarrow$ Holder stores it $\rightarrow$ Holder presents to Verifier $\rightarrow$ Verifier checks Issuer's public key (published on blockchain) to validate the signature. No direct Issuer–Verifier contact needed. (c) The blockchain stores the Issuer's public key (DID document) and revocation status, not personal data. It provides a decentralised, tamper-proof registry so anyone can look up whether the credential is valid and unrevoked.

A3: (a) 1. Cloud backup (encrypted seed phrase stored in iCloud/Google): convenient but relies on a centralised provider. 2. Social recovery (3-of-5 trusted contacts hold key shares): decentralised but requires maintaining trusted relationships. 3. Hardware backup (seed phrase on a steel plate in a safe): very secure but inconvenient and single point of physical loss. (b) Open answer—social recovery balances decentralisation with practicality for most users.