Lesson 8.1 Quiz: Digital Identity and the Data Economy

Module 8: The Future Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Q1: Identity Model Classification

Which identity model requires a **single authority** to issue, store, and verify all identities?

A. Federated identity
B. Self-sovereign identity
C. Centralized identity
D. Decentralized autonomous identity

Q1: Identity Model Classification

Which identity model requires a **single authority** to issue, store, and verify all identities?

- (A) Federated identity
- (B) Self-sovereign identity
- (C) Centralized identity
- (D) Decentralized autonomous identity

Answer: (C) Centralized identity relies on a single authority (e.g., a government or bank) that controls issuance, storage, and verification.

Q2: Federated Identity Advantage

What is the primary advantage of **federated identity** over centralized identity?

A. The user controls all their own data
B. One credential works across multiple services
C. No trust in any third party is required
D. Data is stored on a blockchain

Q2: Federated Identity Advantage

What is the primary advantage of **federated identity** over centralized identity?

- (A) The user controls all their own data
- (B) One credential works across multiple services
- (C) No trust in any third party is required
- (D) Data is stored on a blockchain

Answer: (B) Federated identity allows a single credential (e.g., a bank login) to be accepted across multiple services, reducing duplication. The user still depends on the identity provider.

Q3: SSI Core Principle

Which of the following is a **core principle** of self-sovereign identity (SSI)?

- A government authority must approve every identity transaction
- The individual holds and controls their own credentials
- Identity data is publicly visible on a blockchain
- All identity providers must be banks

Q3: SSI Core Principle

Which of the following is a **core principle** of self-sovereign identity (SSI)?

- (A) A government authority must approve every identity transaction
- (B) The individual holds and controls their own credentials
- (C) Identity data is publicly visible on a blockchain
- (D) All identity providers must be banks

Answer: (B) SSI's defining characteristic is that the individual holds their credentials in a digital wallet and controls what is shared with whom.

Q4: Verifiable Credential Roles

In the verifiable credential "trust triangle," who **creates and signs** the credential?

A. The holder
B. The verifier
C. The issuer
D. The blockchain network

Q4: Verifiable Credential Roles

In the verifiable credential "trust triangle," who **creates and signs** the credential?

A. The holder
B. The verifier
C. The issuer
D. The blockchain network

Answer: (C) The issuer (e.g., a university or bank) creates and cryptographically signs the credential. The holder stores it; the verifier checks it.

Q5: Zero-Knowledge Proof Definition

What does a zero-knowledge proof allow the prover to do?

- A. Reveal all underlying data to the verifier
- B. Convince the verifier a statement is true without revealing any additional information
- C. Encrypt data so that only the government can decrypt it
- D. Store data permanently on a public ledger

Q5: Zero-Knowledge Proof Definition

What does a zero-knowledge proof allow the prover to do?

- (A) Reveal all underlying data to the verifier
- (B) Convince the verifier a statement is true without revealing any additional information
- (C) Encrypt data so that only the government can decrypt it
- (D) Store data permanently on a public ledger

Answer: (B) A ZKP convinces the verifier that a statement (e.g., "age ≥ 18") is true without revealing any information beyond the truth of that statement.

Q6: Data Economy Definition

In the data economy, who typically captures **most of the value** generated from personal data?

A. The individual who generated the data
B. Platforms and data brokers
C. Government regulators
D. Open-source communities

Q6: Data Economy Definition

In the data economy, who typically captures **most of the value** generated from personal data?

- (A) The individual who generated the data
- (B) Platforms and data brokers
- (C) Government regulators
- (D) Open-source communities

Answer: (B) Platforms and data brokers aggregate, analyze, and sell personal data, capturing most of its economic value. Individuals typically receive little or no direct compensation.

Q7: Alternative Data

Which of the following is an example of **alternative data** in finance?

- (A) Quarterly earnings reports filed with regulators
- (B) Satellite imagery of retail parking lots
- (C) A company's audited balance sheet
- (D) Central bank interest rate announcements

Q7: Alternative Data

Which of the following is an example of **alternative data** in finance?

- (A) Quarterly earnings reports filed with regulators
- (B) Satellite imagery of retail parking lots
- (C) A company's audited balance sheet
- (D) Central bank interest rate announcements

Answer: (B) Alternative data includes non-traditional sources like satellite imagery, social media sentiment, and geolocation data. Earnings reports, balance sheets, and central bank data are traditional.

Q8: Differential Privacy Mechanism

How does **differential privacy** protect individual data?

- A. By encrypting all data before analysis
- B. By adding calibrated noise so individuals cannot be identified in aggregate results
- C. By storing data in a secure hardware enclave
- D. By requiring each individual to approve every query

Q8: Differential Privacy Mechanism

How does **differential privacy** protect individual data?

- (A) By encrypting all data before analysis
- (B) By adding calibrated noise so individuals cannot be identified in aggregate results
- (C) By storing data in a secure hardware enclave
- (D) By requiring each individual to approve every query

Answer: (B) Differential privacy adds carefully calibrated random noise to query results, ensuring that aggregate statistics are approximately accurate while individual data points cannot be reverse-engineered.

Q9: ZKP Application

A bank needs to verify that a customer's income exceeds $50,000 for a loan application. Using a zero-knowledge proof, what does the bank learn?

- **A** The customer's exact income and employer name
- **B** Only that the income is above $50,000 (true or false)
- **C** The customer's full tax return
- **D** Nothing — the bank cannot verify anything with ZKPs

Q9: ZKP Application

A bank needs to verify that a customer's income exceeds $50,000 for a loan application. Using a zero-knowledge proof, what does the bank learn?

- (A) The customer's exact income and employer name
- (B) Only that the income is above $50,000 (true or false)
- (C) The customer's full tax return
- (D) Nothing — the bank cannot verify anything with ZKPs

Answer: (B) With a ZKP, the bank learns only the binary answer: "income $>$ $50,000" is true or false. The exact amount, employer, and other details remain private.

Q10: SSI Credential Use Case

A freelancer has a KYC verifiable credential from Bank A. She wants to open an account at Bank B. Under an SSI system, what happens?

A. Bank B must contact Bank A to verify the credential
B. Bank B verifies the credential cryptographically from the freelancer's wallet, without contacting Bank A
C. The freelancer must redo full KYC from scratch at Bank B
D. The government must approve the credential transfer

Q10: SSI Credential Use Case

A freelancer has a KYC verifiable credential from Bank A. She wants to open an account at Bank B. Under an SSI system, what happens?

- (A) Bank B must contact Bank A to verify the credential
- (B) Bank B verifies the credential cryptographically from the freelancer's wallet, without contacting Bank A
- (C) The freelancer must redo full KYC from scratch at Bank B
- (D) The government must approve the credential transfer

Answer: (B) In SSI, verifiable credentials are cryptographically signed by the issuer. Bank B can verify the signature independently without contacting Bank A, making KYC portable.

Q11: Homomorphic Encryption Application

A cloud provider performs credit scoring on **homomorphically encrypted** customer data. What can the cloud provider see?

- (A) All customer data in plaintext during processing
- (B) The customer data in encrypted form only — never the raw data
- (C) Only the final credit score
- (D) Nothing — the computation fails on encrypted data

Q11: Homomorphic Encryption Application

A cloud provider performs credit scoring on **homomorphically encrypted** customer data. What can the cloud provider see?

- (A) All customer data in plaintext during processing
- (B) The customer data in encrypted form only — never the raw data
- (C) Only the final credit score
- (D) Nothing — the computation fails on encrypted data

Answer: (B) Homomorphic encryption allows computation on encrypted data. The cloud provider processes the encrypted data and returns an encrypted result — it never sees the raw customer data.

Q12: SMPC Use Case

Five banks want to build a **joint fraud detection model** using secure multi-party computation. What is the key benefit?

- (A) Each bank shares its raw data with all other banks
- (B) The model is trained on combined data without any bank seeing another's raw data
- (C) Only the largest bank provides data; others benefit for free
- (D) The model is less accurate because data is encrypted

Q12: SMPC Use Case

Five banks want to build a **joint fraud detection model** using secure multi-party computation. What is the key benefit?

- (A) Each bank shares its raw data with all other banks
- (B) The model is trained on combined data without any bank seeing another's raw data
- (C) Only the largest bank provides data; others benefit for free
- (D) The model is less accurate because data is encrypted

Answer: (B) SMPC allows the banks to jointly compute a model using their combined data, but no bank ever sees another bank's raw customer data. The result is a better model with full privacy.

Q13: Privacy Budget

In differential privacy, what happens as the privacy budget (ϵ) **decreases**?

A. Privacy increases and accuracy increases
B. Privacy increases but accuracy decreases
C. Privacy decreases but accuracy increases
D. Privacy and accuracy are unrelated to ϵ

Q13: Privacy Budget

In differential privacy, what happens as the privacy budget (ϵ) **decreases**?

- (A) Privacy increases and accuracy increases
- (B) Privacy increases but accuracy decreases
- (C) Privacy decreases but accuracy increases
- (D) Privacy and accuracy are unrelated to ϵ

Answer: (B) A smaller ϵ means more noise is added, providing stronger privacy guarantees but reducing the accuracy of query results. This is the fundamental trade-off.

Q14: Identity Model Weakness

A major social media platform suffers a data breach exposing 500 million users' login credentials used across dozens of services. Which identity model **most directly** enabled this cascading failure?

- A Centralized identity
- B Federated identity
- C Self-sovereign identity
- D Distributed ledger identity

Q14: Identity Model Weakness

A major social media platform suffers a data breach exposing 500 million users' login credentials used across dozens of services. Which identity model **most directly** enabled this cascading failure?

- (A) Centralized identity
- (B) Federated identity
- (C) Self-sovereign identity
- (D) Distributed ledger identity

Answer: (B) Federated identity ("Login with Platform X") creates a single credential used across many services. When the identity provider is breached, all relying services are compromised.

Q15: Consent Problem

Why is "informed consent" considered largely fictional in the current data economy?

A. Privacy policies are written in clear, simple language
B. Users have ample time to read and understand all terms
C. Privacy policies are too long and complex for realistic human comprehension
D. Consent is never required under any jurisdiction

Q15: Consent Problem

Why is "informed consent" considered largely fictional in the current data economy?

- (A) Privacy policies are written in clear, simple language
- (B) Users have ample time to read and understand all terms
- (C) Privacy policies are too long and complex for realistic human comprehension
- (D) Consent is never required under any jurisdiction

Answer: (C) Studies estimate that reading all privacy policies a user encounters would take 76+ working days per year. The information asymmetry makes genuine "informed" consent practically impossible.

Q16: Alternative Data Ethics

A hedge fund buys anonymized credit card transaction data to predict retail company revenues before earnings are reported. Which concern is **most relevant**?

- A The data is too expensive for the hedge fund
- B Consumers did not consent to their spending data being used for investment analysis
- C The hedge fund is required to share its trading profits with consumers
- D Anonymized data has no privacy implications

Q16: Alternative Data Ethics

A hedge fund buys anonymized credit card transaction data to predict retail company revenues before earnings are reported. Which concern is **most relevant**?

- (A) The data is too expensive for the hedge fund
- (B) Consumers did not consent to their spending data being used for investment analysis
- (C) The hedge fund is required to share its trading profits with consumers
- (D) Anonymized data has no privacy implications

Answer: (B) Even when anonymized, consumers typically did not consent to their transaction data being sold to hedge funds for investment purposes. This raises serious consent and ethical concerns.

Q17: TEE Limitation

What is the primary limitation of Trusted Execution Environments (TEEs) compared to purely mathematical privacy techniques?

- A. TEEs are always slower than homomorphic encryption
- B. TEEs require trust in the hardware manufacturer
- C. TEEs cannot perform any computation
- D. TEEs expose all data to the operating system

Q17: TEE Limitation

What is the primary limitation of Trusted Execution Environments (TEEs) compared to purely mathematical privacy techniques?

- (A) TEEs are always slower than homomorphic encryption
- (B) TEEs require trust in the hardware manufacturer
- (C) TEEs cannot perform any computation
- (D) TEEs expose all data to the operating system

Answer: (B) TEEs rely on hardware for security, meaning you must trust the chip manufacturer. Mathematical techniques (ZKP, SMPC, homomorphic encryption) provide security based on mathematical proofs, independent of hardware trust.

Q18: Utility–Privacy Trade-off

A regulator proposes banning all use of personal financial data for credit scoring to protect privacy. What is the **most likely unintended consequence**?

- (A) Credit becomes more accessible to underserved populations
- (B) Lenders cannot assess risk, leading to higher interest rates or reduced lending
- (C) Data brokers will voluntarily stop collecting data
- (D) Privacy-preserving technologies become unnecessary

Q18: Utility–Privacy Trade-off

A regulator proposes banning all use of personal financial data for credit scoring to protect privacy. What is the **most likely unintended consequence**?

- (A) Credit becomes more accessible to underserved populations
- (B) Lenders cannot assess risk, leading to higher interest rates or reduced lending
- (C) Data brokers will voluntarily stop collecting data
- (D) Privacy-preserving technologies become unnecessary

Answer: (B) Without personal financial data, lenders cannot differentiate risk. This leads to adverse selection: higher rates for everyone, reduced lending, or exclusion of borderline borrowers — harming the very populations regulation aims to protect.

Q19: eIDAS 2.0 Impact

If the EU Digital Identity Wallet achieves widespread adoption, which existing industry is **most disrupted**?

- A. The cryptocurrency mining industry
- B. The identity verification and KYC service provider industry
- C. The stock exchange industry
- D. The insurance claims processing industry

Q19: eIDAS 2.0 Impact

If the EU Digital Identity Wallet achieves widespread adoption, which existing industry is **most disrupted**?

- (A) The cryptocurrency mining industry
- (B) The identity verification and KYC service provider industry
- (C) The stock exchange industry
- (D) The insurance claims processing industry

Answer: (B) A government-backed digital identity wallet that provides instant, portable KYC directly threatens the multi-billion-euro identity verification industry that currently charges banks per verification.

Q20: Technology Selection

A consortium of three banks wants to jointly detect money laundering patterns across their combined customer data. They need exact results (no noise), reasonable performance, and no bank should see another's data. Which privacy technique is **best suited**?

- A Differential privacy
- B Homomorphic encryption
- C Secure multi-party computation (SMPC)
- D Simple data anonymization

Q20: Technology Selection

A consortium of three banks wants to jointly detect money laundering patterns across their combined customer data. They need exact results (no noise), reasonable performance, and no bank should see another's data. Which privacy technique is **best suited**?

- (A) Differential privacy
- (B) Homomorphic encryption
- (C) Secure multi-party computation (SMPC)
- (D) Simple data anonymization

Answer: (C) SMPC is designed for multi-party joint computation with exact results and no data sharing. Differential privacy adds noise (inexact). Homomorphic encryption is too slow. Anonymization does not prevent re-identification.