Lesson 8.1 Quiz: Digital Identity and the Data Economy

Module 8: The Future Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course (v2026.05)

Q1: Identity Model Classification

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

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

Q1: Identity Model Classification

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q2: Federated Identity Advantage

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

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

Q2: Federated Identity Advantage

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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. Identity data is publicly visible on a blockchain
C. All identity providers must be banks
D. The individual holds and controls their own credentials

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
- Identity data is publicly visible on a blockchain
- All identity providers must be banks
- The individual holds and controls their own credentials

[Answer hidden – compile with \solutionstrue to reveal]

Q4: Verifiable Credential Roles

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

- (A) The blockchain network
- (B) The verifier
- (C) The issuer
- (D) The holder

Q4: Verifiable Credential Roles

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

- (A) The blockchain network
- (B) The verifier
- (C) The issuer
- (D) The holder

[Answer hidden – compile with \solutionstrue to reveal]

Q5: Zero-Knowledge Proof Definition

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

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

Q5: Zero-Knowledge Proof Definition

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q6: Data Economy Definition

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

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

Q6: Data Economy Definition

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q7: Alternative Data

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

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

Q7: Alternative Data

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q8: Differential Privacy Mechanism

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

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

Q8: Differential Privacy Mechanism

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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 hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q13: Privacy Budget

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

[Answer hidden – compile with \solutionstrue to reveal]

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 Privacy policies are too long and complex for realistic human comprehension
- C Consent is never required under any jurisdiction
- D Users have ample time to read and understand all terms

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** Privacy policies are too long and complex for realistic human comprehension
- **C** Consent is never required under any jurisdiction
- **D** Users have ample time to read and understand all terms

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q17: TEE Limitation

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

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

Q17: TEE Limitation

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]

Q19: eIDAS 2.0 Impact

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

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

Q19: eIDAS 2.0 Impact

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

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

[Answer hidden – compile with \solutionstrue to reveal]

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

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

[Answer hidden – compile with \solutionstrue to reveal]