Lesson 6.3: API Economy and Platform Architecture – Quiz

Prof. Dr. Joerg Osterrieder

Question 1

What does API stand for, and what is its primary purpose in financial services?

A. Application Programming Interface; it defines how two software systems communicate
B. Advanced Processing Infrastructure; it speeds up batch processing
C. Automated Payment Interface; it replaces human tellers
D. Account Payment Instruction; it encodes wire transfer details

Question 1

What does API stand for, and what is its primary purpose in financial services?

A. Application Programming Interface; it defines how two software systems communicate

B. Advanced Processing Infrastructure; it speeds up batch processing

C. Automated Payment Interface; it replaces human tellers

D. Account Payment Instruction; it encodes wire transfer details

[Answer hidden – compile with \solutionstrue to reveal]
An API is a contract specifying endpoints, request/response formats, authentication, and error codes. In finance, APIs enable third parties to access bank data and initiate payments programmatically.

Question 2

Which API style is best suited for a fintech dashboard that needs to display data from accounts, cards, and loans in a single page load?

A. GraphQL, because the client can request exactly the fields it needs across multiple entities in one query
B. REST, because each resource has its own endpoint
C. SOAP, because it guarantees ACID transactions
D. Webhooks, because the server pushes updates

Question 2

Which API style is best suited for a fintech dashboard that needs to display data from accounts, cards, and loans in a single page load?

A. GraphQL, because the client can request exactly the fields it needs across multiple entities in one query

B. REST, because each resource has its own endpoint

C. SOAP, because it guarantees ACID transactions

D. Webhooks, because the server pushes updates

[Answer hidden – compile with \solutionstrue to reveal]

GraphQL lets the client specify exactly which fields from accounts, cards, and loans it needs in a single request, avoiding the over-fetching and multiple round-trips typical of REST.

Question 3

What are the two new roles created by PSD2?

A. Market Maker and Market Taker
B. Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP)
C. Data Controller and Data Processor (GDPR roles)
D. Core Banking Provider (CBP) and Cloud Service Provider (CSP)

Question 3

What are the two new roles created by PSD2?

A. Market Maker and Market Taker

B. Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP)

C. Data Controller and Data Processor (GDPR roles)

D. Core Banking Provider (CBP) and Cloud Service Provider (CSP)

[Answer hidden – compile with \solutionstrue to reveal]
PSD2 created AISPs (read account data) and PISPs (initiate payments) as licensed third-party roles that can access bank systems via standardized APIs with customer consent.

Question 4

A customer uses a budgeting app that shows balances from three different banks. Which PSD2 service is the app using?

A. BaaS (Banking-as-a-Service) – it provides a full banking stack
B. SCA (Strong Customer Authentication) – it verifies the customer's identity
C. PIS (Payment Initiation Service) – it initiates transfers between accounts
D. AIS (Account Information Service) – it reads account data with consent

Question 4

A customer uses a budgeting app that shows balances from three different banks. Which PSD2 service is the app using?

A. BaaS (Banking-as-a-Service) – it provides a full banking stack

B. SCA (Strong Customer Authentication) – it verifies the customer's identity

C. PIS (Payment Initiation Service) – it initiates transfers between accounts

D. AIS (Account Information Service) – it reads account data with consent

[Answer hidden – compile with \solutionstrue to reveal]
Reading balances and transactions from multiple banks is an Account Information Service. The app is a licensed AISP that aggregates data via open banking APIs with the customer's explicit consent.

Question 5

What is the main improvement PSD3/PSR brings over PSD2?

A. It removes the requirement for customer consent
B. It prohibits third-party access to bank data
C. It mandates API performance standards (latency, uptime SLAs) and extends data access beyond payments
D. It replaces REST APIs with blockchain-based communication

Question 5

What is the main improvement PSD3/PSR brings over PSD2?

A. It removes the requirement for customer consent

B. It prohibits third-party access to bank data

C. It mandates API performance standards (latency, uptime SLAs) and extends data access beyond payments

D. It replaces REST APIs with blockchain-based communication

[Answer hidden – compile with \solutionstrue to reveal]
PSD3 moves from "banks must offer APIs" to "banks must offer *good* APIs" with performance SLAs. The companion FiDA regulation extends open data to insurance, pensions, and investments.

Question 6

Which of the following is NOT a core function of an API gateway?

A. Enforcing authentication and rate limiting
B. Logging API usage for analytics and audit
C. Executing the business logic of each financial transaction
D. Routing requests to the correct internal microservice

Question 6

Which of the following is NOT a core function of an API gateway?

A. Enforcing authentication and rate limiting

B. Logging API usage for analytics and audit

C. Executing the business logic of each financial transaction

D. Routing requests to the correct internal microservice

[Answer hidden – compile with \solutionstrue to reveal]
The API gateway handles cross-cutting concerns (routing, auth, rate limiting, logging) but does NOT execute business logic. Business logic resides in the backend microservices behind the gateway.

Question 7

Why is rate limiting important for banking APIs?

A. It increases the speed of API responses
B. It replaces the need for authentication
C. It ensures all API consumers pay the same price
D. It prevents abuse, DDoS attacks, and runaway scripts from overwhelming backend systems

Question 7

Why is rate limiting important for banking APIs?

A. It increases the speed of API responses

B. It replaces the need for authentication

C. It ensures all API consumers pay the same price

D. It prevents abuse, DDoS attacks, and runaway scripts from overwhelming backend systems

[Answer hidden – compile with \solutionstrue to reveal]
Rate limiting caps the number of API calls per client per time window, protecting backend systems from overload. It is a critical layer of defence, not a replacement for authentication.

Question 8

In OAuth 2.0, what is the purpose of the access token?

A. It stores the user's bank password in encrypted form

B. It grants the third-party app time-limited, scoped access to the user's bank data without exposing credentials

C. It replaces the need for TLS encryption

D. It permanently links the user's identity to the third-party app

Question 8

In OAuth 2.0, what is the purpose of the access token?

A. It stores the user's bank password in encrypted form

B. It grants the third-party app time-limited, scoped access to the user's bank data without exposing credentials

C. It replaces the need for TLS encryption

D. It permanently links the user's identity to the third-party app

[Answer hidden – compile with \solutionstrue to reveal]
An access token is a short-lived credential that grants specific permissions (scopes) to a third-party app. The user's password is never shared with the third party. Tokens typically expire in 5–60 minutes.

Question 9

What does mTLS add beyond standard TLS?

A. It encrypts the data payload twice
B. It compresses API responses for faster transmission
C. It requires the client (not just the server) to present a certificate, enabling mutual identity verification
D. It removes the need for OAuth tokens

Question 9

What does mTLS add beyond standard TLS?

A. It encrypts the data payload twice

B. It compresses API responses for faster transmission

C. It requires the client (not just the server) to present a certificate, enabling mutual identity verification

D. It removes the need for OAuth tokens

[Answer hidden – compile with \solutionstrue to reveal]
Standard TLS only authenticates the server. Mutual TLS (mTLS) requires both parties to present certificates, creating a cryptographic chain of trust. PSD2 requires mTLS for AISP/PISP bank communication.

Question 10

How does Banking-as-a-Service (BaaS) differ from open banking?

A. BaaS is regulation-driven; open banking is market-driven

B. Open banking provides a full banking license; BaaS does not

C. BaaS provides the full banking stack (accounts, cards, lending) via proprietary APIs; open banking is regulation-driven and mostly read-only

D. There is no difference; the terms are interchangeable

Question 10

How does Banking-as-a-Service (BaaS) differ from open banking?

A. BaaS is regulation-driven; open banking is market-driven

B. Open banking provides a full banking license; BaaS does not

C. BaaS provides the full banking stack (accounts, cards, lending) via proprietary APIs; open banking is regulation-driven and mostly read-only

D. There is no difference; the terms are interchangeable

[Answer hidden – compile with \solutionstrue to reveal]
Open banking is regulation-driven (PSD2) and primarily covers account data and payment initiation. BaaS is market-driven and exposes the full banking stack—accounts, cards, lending, compliance—via proprietary APIs.

Question 11

The Synapse BaaS provider collapsed in 2024 with $85M in unreconciled customer funds. What was the root cause?

A. A cyberattack that drained customer accounts
B. Customers withdrew all funds simultaneously (bank run)
C. Synapse's virtual ledger diverged from the partner bank's ledger, making funds unreconcilable
D. The partner bank revoked all API access without notice

Question 11

The Synapse BaaS provider collapsed in 2024 with $85M in unreconciled customer funds. What was the root cause?

A. A cyberattack that drained customer accounts

B. Customers withdrew all funds simultaneously (bank run)

C. Synapse's virtual ledger diverged from the partner bank's ledger, making funds unreconcilable

D. The partner bank revoked all API access without notice

[Answer hidden – compile with \solutionstrue to reveal]
Synapse maintained a shadow ledger that diverged from Evolve Bank's records. When Synapse failed, no one could determine which customers owned which funds. This exposed the chain-of-custody risk in BaaS models.

Question 12

What is embedded finance?

A. A banking app embedded in a mobile phone's operating system

B. Financial services integrated into non-financial products and customer journeys, so the user never leaves the host platform

C. A physical bank branch located inside a retail store

D. A financial database embedded in a blockchain

Question 12

What is embedded finance?

A. A banking app embedded in a mobile phone's operating system

B. Financial services integrated into non-financial products and customer journeys, so the user never leaves the host platform

C. A physical bank branch located inside a retail store

D. A financial database embedded in a blockchain

[Answer hidden – compile with \solutionstrue to reveal]
Embedded finance integrates payments, lending, or insurance into non-financial platforms (e.g., Shopify Capital offering loans inside the e-commerce dashboard). Finance becomes invisible infrastructure.

Question 13

Which of the following is an example of embedded finance?

A. A bank sending a paper statement to a customer's home address
B. A customer visiting a bank branch to apply for a mortgage
C. A customer downloading a separate banking app to check their balance
D. Shopify offering business loans directly in its merchant dashboard, powered by a BaaS provider

Question 13

Which of the following is an example of embedded finance?

A. A bank sending a paper statement to a customer's home address

B. A customer visiting a bank branch to apply for a mortgage

C. A customer downloading a separate banking app to check their balance

D. Shopify offering business loans directly in its merchant dashboard, powered by a BaaS provider

[Answer hidden – compile with \solutionstrue to reveal]
Shopify Capital is a textbook embedded finance example: a non-financial platform (e-commerce) offers financial services (lending) at the moment of need, powered by BaaS APIs, without the merchant leaving Shopify.

Question 14

What creates network effects in a financial API platform like Stripe?

A. More developers building on Stripe attracts more merchants, which generates more payment volume and better fraud models, which attracts more developers

B. Stripe holds a banking license in every country

C. Stripe charges lower fees than competitors

D. Stripe uses blockchain for all transactions

Question 14

What creates network effects in a financial API platform like Stripe?

A. More developers building on Stripe attracts more merchants, which generates more payment volume and better fraud models, which attracts more developers

B. Stripe holds a banking license in every country

C. Stripe charges lower fees than competitors

D. Stripe uses blockchain for all transactions

[Answer hidden – compile with \solutionstrue to reveal]
Network effects create a virtuous cycle: more developers → more merchants → more payment data → better fraud detection → higher approval rates → more developers. This is a multi-sided platform dynamic.

Question 15

What is a "take rate" in the context of financial platforms?

A. The rate at which APIs respond to requests (latency)
B. The interest rate a platform charges on loans
C. The rate at which customers adopt a new banking app
D. The percentage of transaction value captured by the platform as revenue

Question 15

What is a "take rate" in the context of financial platforms?

A. The rate at which APIs respond to requests (latency)

B. The interest rate a platform charges on loans

C. The rate at which customers adopt a new banking app

D. The percentage of transaction value captured by the platform as revenue

[Answer hidden – compile with \solutionstrue to reveal]
Take rate is the core monetization metric for platforms. Stripe's take rate is approximately 2.9% + \$0.30 per transaction. Higher take rates mean more revenue per dollar flowing through the platform.

Question 16

Why did Stripe win the payments market despite not being the cheapest option?

A. Stripe had the best marketing budget

B. Stripe offered the best developer experience (DX): clear docs, SDKs, sandbox, and 7 lines of code to accept a payment

C. Stripe held more banking licenses than competitors

D. Stripe was the first company to offer online payments

Question 16

Why did Stripe win the payments market despite not being the cheapest option?

A. Stripe had the best marketing budget

B. Stripe offered the best developer experience (DX): clear docs, SDKs, sandbox, and 7 lines of code to accept a payment

C. Stripe held more banking licenses than competitors

D. Stripe was the first company to offer online payments

[Answer hidden – compile with \solutionstrue to reveal]
Stripe's competitive advantage was developer experience: the fastest time-to-first-API-call, the best documentation, and SDKs in every major language. DX is the primary competitive differentiator for API platforms.

Question 17

Which of the following is a DX anti-pattern commonly seen in traditional banks?

A. Requiring a sales call and NDA before developers can access API documentation
B. Providing a sandbox environment with realistic test data
C. Providing an interactive API explorer with Swagger/OpenAPI
D. Offering SDKs in multiple programming languages

Question 17

Which of the following is a DX anti-pattern commonly seen in traditional banks?

A. Requiring a sales call and NDA before developers can access API documentation

B. Providing a sandbox environment with realistic test data

C. Providing an interactive API explorer with Swagger/OpenAPI

D. Offering SDKs in multiple programming languages

[Answer hidden – compile with \solutionstrue to reveal]
Gating API documentation behind sales calls is a major friction point that drives developers to competitors. Best practice is self-service sign-up with immediate sandbox access and time-to-first-call under 5 minutes.

Question 18

In the "defence in depth" security model for financial APIs, which layer does OAuth 2.0 operate at?

A. Application layer (authorization)
B. Data layer (field-level encryption)
C. Network layer (firewalls, IP allowlisting)
D. Transport layer (TLS encryption)

Question 18

In the "defence in depth" security model for financial APIs, which layer does OAuth 2.0 operate at?

A. Application layer (authorization)
B. Data layer (field-level encryption)
C. Network layer (firewalls, IP allowlisting)
D. Transport layer (TLS encryption)

[Answer hidden – compile with \solutionstrue to reveal]
OAuth 2.0 operates at the application layer, handling authorization (who can access what). mTLS operates at the transport layer. Firewalls at the network layer. Each layer provides independent protection.

Question 19

A fintech startup is choosing between building its own banking infrastructure and using a BaaS provider. The startup needs to launch in 3 months with limited capital. Which strategy is most appropriate?

A. Wait for PSD3 to be finalized before launching

B. Use a BaaS provider for fast time-to-market, but plan multi-provider redundancy to mitigate vendor risk

C. Apply for a banking license and build from scratch

D. Build everything in-house for maximum control

Question 19

A fintech startup is choosing between building its own banking infrastructure and using a BaaS provider. The startup needs to launch in 3 months with limited capital. Which strategy is most appropriate?

A. Wait for PSD3 to be finalized before launching

B. Use a BaaS provider for fast time-to-market, but plan multi-provider redundancy to mitigate vendor risk

C. Apply for a banking license and build from scratch

D. Build everything in-house for maximum control

[Answer hidden – compile with \solutionstrue to reveal]

With limited time and capital, BaaS provides the fastest path to market. However, the Synapse collapse demonstrates the importance of multi-provider redundancy and not depending on a single middleware vendor.

Question 20

What is the key lesson from the Synapse collapse for the BaaS industry?

A. BaaS is inherently unsafe and should be banned

B. Fintechs should always hold their own banking license

C. Middleware providers should maintain independent ledgers separate from the bank

D. The licensed bank is ultimately responsible for customer funds; middleware must not create shadow accounting that can diverge from the bank's records

Question 20

What is the key lesson from the Synapse collapse for the BaaS industry?

A. BaaS is inherently unsafe and should be banned

B. Fintechs should always hold their own banking license

C. Middleware providers should maintain independent ledgers separate from the bank

D. The licensed bank is ultimately responsible for customer funds; middleware must not create shadow accounting that can diverge from the bank's records

[Answer hidden – compile with \solutionstrue to reveal]
The Synapse collapse showed that when middleware maintains its own "virtual ledger" that diverges from the bank's books, customer funds become unreconcilable. Ledger integrity and regulatory clarity on responsibility are essential.