Implementation Models for Banks in the Context of the Digital Euro

A technical and organisational thesis on integration architectures, shared services, and bank-tier-specific implementation strategies

<Your Name>
<Department / Faculty>
<University>

January 24, 2026

Abstract

The potential introduction of a retail digital euro introduces a new payment rail whose operational model combines Eurosystem-provided scheme components with bank- or payment service provider (PSP)-implemented distribution, customer servicing, and compliance capabilities. This thesis develops a technical reference architecture and a set of bank-tier-specific implementation models (in-house, hybrid, outsourced) for integrating the digital euro into existing bank payment ecosystems. The work is grounded in official Eurosystem documentation (rulebook development and preparation-phase materials), the Eurosystem innovation platform/experimentation portal interfaces, and industry cost studies. It proposes a modular decomposition of affected bank components (channels, payment hubs, customer identity, liquidity, compliance, acceptance infrastructure), distinguishes components that can be mutualised across PSPs (shared integration) from those that should remain bank-specific, and evaluates architectural patterns (monolithic, modular monolith, microservices/event-driven) in terms of time-to-market, cost, resilience, and regulatory fit. A multi-criteria decision analysis (MCDA) and scenario-based cost model are used to map appropriate implementation strategies to bank tiers defined by size and operational complexity. The thesis concludes with actionable blueprints and a migration roadmap for banks and PSP consortia, emphasising cost mutualisation opportunities and robust governance aligned with the digital euro scheme rulebook.

Keywords

Digital euro; CBDC; payment systems; banking architecture; interoperability; shared services; outsourcing; microservices; access gateway; rulebook; cost mutualisation.

Contents

List of Figures

List of Tables

Abbreviations

Term	Meaning
CBDC	Central Bank Digital Currency
ECB	European Central Bank
Eurosystem	ECB + national central banks of the euro area
PSP	Payment Service Provider
DESP	Digital Euro Service Platform (term used for Eurosystem service platform)
DCA	Dedicated Cash Account (liquidity account concept for intermediaries)
API	Application Programming Interface
HSM	Hardware Security Module
DORA	Digital Operational Resilience Act
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
KYC	Know Your Customer
SCA	Strong Customer Authentication
POS	Point of Sale
ATM	Automated Teller Machine

Chapter 1

Introduction

1.1 Context and motivation

The digital euro is envisaged as a digital form of central bank money, complementing cash and enabling electronic payments in shops, online, and peer-to-peer across the euro area (**ecb_digital_euro_page**). Its introduction is framed as a strategic response to shifts in the payment landscape (including the growing role of non-European payment infrastructures) and aims to preserve the role of central bank money as an anchor for the payment system (**ecb_digital_euro_page**). In parallel, EU co-legislators have advanced legal-framework discussions; for example, the Council of the EU agreed a negotiating position that emphasises that a digital euro would complement cash and be usable across the euro area (**eu_council_2025_digital_euro_position**).

From a bank/PSP perspective, the digital euro is not a mere "new instrument" added to existing channels. Rather, it introduces a new interoperability surface (to the Eurosystem service platform) and a new set of scheme rules, technical standards, operational procedures, and customer-service obligations. Implementation decisions will materially affect cost, delivery risk, and the ability to reuse resulting capabilities for private-sector payment innovation (e.g., pan-European wallet propositions). A central challenge is that banks are heterogeneous: they differ in IT maturity, channel footprints, sourcing strategies, and governance structures. Consequently, a one-size-fits-all integration approach is unlikely to be cost-optimal or operationally resilient.

1.2 Problem statement

Banks must integrate the digital euro into existing payment ecosystems while maintaining service continuity, security, compliance, and cost discipline. The integration touches multiple layers: customer channels (mobile apps, cards, branch/ATM), payment processing and orchestration, customer identity and access management, liquidity/funding mechanics,

compliance and risk controls, reporting, and merchant acceptance infrastructure. Industry studies suggest substantial investment may be required if implemented in a stand-alone or non-mutualised manner (**pwc_coststudy_2025**). At the same time, Eurosystem assessments highlight significant potential for cost mutualisation through shared solutions and external synergies, implying that banks need not implement digital euro capabilities entirely on their own (**ecb_costs_2025**).

1.3 Research objectives and questions

Guided by the attached research outline (user-provided), this thesis addresses the following research questions (RQs):

RQ1: How can banks technically integrate the digital euro into existing architectures, and what are the principal integration patterns?

RQ2: Which capabilities are provided by the Eurosystem (scheme/DESP) versus those to be implemented by intermediaries (banks/PSPs)?

RQ3: Which bank/PSP modules are affected by digital euro integration, and how can these be decomposed into reusable components?

RQ4: Which integration components can be mutualised/shared across PSPs (software and hardware), and which must remain bank-specific?

RQ5: Which implementation model (in-house, hybrid, outsourced) is appropriate for different bank tiers, considering cost, risk, and time-to-market?

1.4 Contributions

The thesis makes five contributions:

1. A **rulebook-aligned reference architecture** that maps scheme functions to bank modules and integration interfaces.
2. A **bank/PSP module impact model**, linking functional domains (access, transaction, liquidity, offline, acceptance) to internal components.
3. A **shared vs. dedicated integration taxonomy** across software and hardware (e.g., gateways, offline devices, acceptance utilities).
4. A **bank-tier-specific implementation model matrix** (in-house / hybrid / outsourced) with MCDA scoring and decision rules.

5. A **scenario-based cost and resource analysis** synthesising public cost studies and synergy mechanisms.

1.5 Scope and assumptions

The work focuses on retail digital euro distribution by banks and PSPs in the euro area context. It is concerned with integration architecture and operating models rather than macroeconomic impacts. Where rulebook details remain under development, the thesis uses published preparation-phase and rulebook development updates and clearly states assumptions (**ecb_closing_report_2025**; **ecb_rdg_progress_2025**).

Chapter 2

Background: Digital euro scheme and platform

2.1 Scheme governance and rulebook structure

The Eurosystem has organised rulebook development through a Rulebook Development Group (RDG), aiming to provide a single set of rules and standards for intermediaries and the ecosystem (**ecb_costs_2025**; **ecb_rdg_progress_2025**). The preparation phase documentation indicates that the scheme rulebook is intended to specify roles, responsibilities, operational procedures, and technical standards necessary for uniform implementation (**ecb_closing_report_2025**).

2.1.1 Functional domains

In order to align the thesis with the scheme's structure, we use the following domain breakdown as organising principle throughout Chapters 4–9:

- **Access management**: onboarding, authentication, device binding, credential lifecycle, and access policies.
- **Transaction management**: payment initiation, authorisation, execution, reversals, dispute primitives, and status tracking.
- **Liquidity management**: DCA funding/defunding, limits enforcement, and treasury interfaces.
- **Alias and reference data**: lookup/portability, identifiers, and scheme reference data.
- **Settlement and reporting**: settlement-related interactions, fee/reporting interfaces (including Eurosystem-provided functions).

- **Offline and conditional/value-added features**: offline synchronisation, conditional payments, and programmable services layered on acceptance standards.

2.2 Intermediary role and the "access gateway" concept

Industry guidance highlights that intermediaries (banks/PSPs) connect to the digital euro service platform through an *access gateway* that acts as a single point of contact, abstracting/hiding backend components behind a unified interface (**eba_guide_2023**). This design aligns with the principle of reducing integration coupling by providing a stable interface boundary between intermediaries and the Eurosystem platform, supporting both interoperability and evolvability.

2.3 Digital euro channels and acceptance ecosystem

The digital euro is intended to support payments in physical POS, e-commerce, and P2P contexts (**ecb_digital_euro_page**). National central banks communicate the project as a complement to cash with broad usability and strong safety properties (**bundesbank_digital_euro_2025**). From an intermediary perspective, channel integration involves: (i) consumer-facing wallets or wallet capabilities integrated into existing banking apps, (ii) merchant acceptance enablement (POS terminal updates, payment pages, QR/NFC interaction), and (iii) cash-like access paths such as branch/ATM interfaces for onboarding and funding/defunding (**pwc_coststudy_2025**).

2.4 Innovation platform and experimentation portal

The preparation phase included an innovation platform in which market participants tested use cases and interfaces, including conditional-payment features and e-commerce/payment initiation scenarios (**ecb_closing_report_2025**; **ecb_innovation_annex_2025**). The experimentation portal supports both synchronous REST APIs and gRPC interfaces; implementation specifications include REST due to market preference while supporting gRPC for broader ecosystem compatibility (**ecb_innovation_annex_2025**).

Chapter 3

Related work and literature review

3.1 CBDC integration architectures

CBDC technical literature commonly distinguishes between (a) core ledger and issuance infrastructure, typically central bank-operated, and (b) intermediary distribution layers providing wallets, KYC, customer service, and value-added features. For the digital euro, this aligns with the access-gateway model and intermediary responsibilities as described in industry guidance and Eurosystem documents (**eba_guide_2023**; **ecb_closing_report_2025**).

3.2 Payment industry mutualisation

The payment industry historically relies on shared infrastructures (clearing/settlement utilities, scheme processors, shared compliance tooling). The ECB cost assessment explicitly notes that banks already use shared solutions for payment channels, accounts, compliance, and operational support, and argues similar approaches can be applied to digital euro integration (**ecb_costs_2025**). This provides a foundation for modelling shared vs. dedicated modules in this thesis.

3.3 Cost evidence and concerns

A prominent industry study estimates that participating banks could face over 2 billion in introduction costs (panel of 19 banks), with an extrapolated euro-area figure of 18 billion, and indicates that the technical layer constitutes around 75% of cost (**pwc_coststudy_2025**). In contrast, the ECB cost note suggests that once cost mutualisation and synergies are accounted for, total costs could fall in a range of 4–5.77 billion over four years (**ecb_costs_2025**). This gap motivates systematic identification of mutualisable components and bank-tier-specific operating models.

3.4 Gap analysis

Existing publications provide (i) high-level descriptions of digital euro objectives and status (**ecb_digital_euro_page**; **eu_council_2025_digital_euro_position**), (ii) industry guidance on intermediary roles and access gateway concepts (**eba_guide_2023**), and (iii) cost estimates with different assumptions (**pwc_coststudy_2025**; **ecb_costs_2025**). However, there is limited publicly available work translating these into an actionable, rulebook-aligned reference architecture and decision framework mapping implementation models to bank tiers. This thesis addresses that gap.

Chapter 4

Methodology

4.1 Research design

The thesis combines **design science** and **applied systems engineering**. The artefacts are (a) a reference architecture, (b) implementation model matrix, and (c) decision and cost analysis tools. Evidence is derived from document analysis of Eurosystem publications and industry studies, and synthesis into architectural patterns.

4.2 Data sources

Primary sources include:

- Eurosystem/ECB rulebook and preparation-phase materials (**ecb_closing_report_2025**; **ecb_rdg_progress_2025**; **ecb_innovation_annex_2025**);
- Industry guidance for banks on the digital euro (**eba_guide_2023**);
- Public cost studies and cost-synergy analysis (**pwc_coststudy_2025**; **ecb_costs_2025**);
- Sector IT survey evidence for outsourcing and IT spend profiles (contextual) (**cipa_rilevazione_it_2025**).

4.3 Analytical framework

Two complementary analyses are applied:

4.3.1 (A) Module decomposition and sharing potential

We decompose end-to-end digital euro capabilities into modules, then classify each module as:

- **Mutualisable**: can be shared across banks/PSPs (e.g., via a utility or vendor) with limited loss of differentiation.
- **Group-shared**: mutualisable within a banking group, IPS, or cooperative structure.
- **Bank-specific**: must remain within each bank due to customer relationship, risk appetite, data constraints, or strategic differentiation.

The ECB cost note provides an analytical basis and empirical synergy factors for market-wide and group-level mutualisation (**ecb_costs_2025**).

4.3.2 (B) Multi-criteria decision analysis (MCDA)

Implementation options (in-house, hybrid, outsourced) are evaluated per bank tier using MCDA with criteria: time-to-market, CapEx, OpEx, integration risk, security/compliance, operational resilience, vendor lock-in, scalability, and reuse potential. Weights are selected to reflect typical supervisory and strategic priorities; sensitivity analysis is included.

4.4 Bank tiering model

We define bank tiers in line with size clusters used in cost evidence (assets brackets) (**pwc_coststudy_2025**; **ecb_costs_2025**):

- **Tier 1 (Top)**: total assets $>$ 1 trillion.
- **Tier 2 (Large)**: 100 billion – 1 trillion.
- **Tier 3 (Mid)**: 30 billion – 100 billion.
- **Tier 4 (Small)**: $<$ 30 billion.

This is a practical proxy for organisational scale, channel footprint (ATM/branch/POS), and engineering capacity.

Chapter 5

Technical integration: reference architecture

5.1 High-level integration landscape

Figure **??** provides a rulebook-aligned high-level architecture. Intermediaries integrate via a dedicated *Digital Euro Integration Layer* (DEIL) that encapsulates protocol adapters (REST/gRPC), security controls, and business orchestration, and connects internal systems and channels to the access gateway.

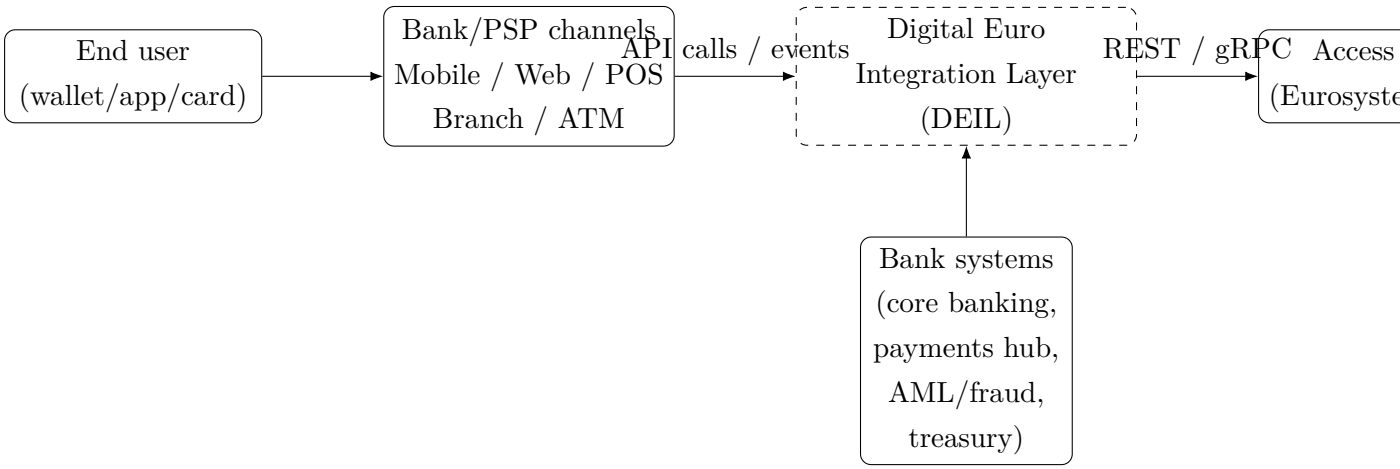

Figure 5.1: Reference architecture: intermediary integration via a Digital Euro Integration Layer (DEIL) and the access gateway.

5.2 Protocol and security interface patterns

The experimentation portal supports REST and gRPC interfaces; REST is a synchronous interface selected in implementation specifications due to market preference, while gRPC is supported for broader compatibility (**ecb_innovation_annex_2025**). For REST, the portal uses HTTP Basic Authentication and requires request signatures for state-changing methods (e.g., POST/PUT), while GET requests do not require signatures (**ecb_innovation_annex_2025**).

5.2.1 Security controls and key management

A production-grade integration requires layered controls:

- **Transport security**: mutual TLS and network segmentation.
- **Request authentication**: BasicAuth (or production equivalent) plus signed requests where applicable (**ecb_innovation_annex_2025**).
- **Non-repudiation**: signing keys protected by HSMs; auditable signature verification logs.
- **Authorisation**: policy enforcement (scopes, roles, device binding) aligned with access management domain.
- **Observability**: centralised logging, distributed tracing, anomaly detection.

5.2.2 Example request-signing envelope (illustrative)

Listing 5.1: Illustrative JSON envelope for signed request payloads (conceptual).

```
{
  "header": {
    "requestId": "uuid",
    "timestamp": "2026-01-24T10:15:30Z",
    "clientId": "bank-psp-id",
    "signature": "base64(signature_over_canonical_payload)"
  },
  "body": {
    "operation": "initiatePayment",
    "amount": "10.00",
    "currency": "EUR",
    "payee": { "alias": "merchant-xyz" },
    "payer": { "walletId": "..." }
  }
```

```
}
```

5.3 Functional flows

5.3.1 Online payment flow (conceptual sequence)

Figure **??** sketches an online payment flow, abstracting scheme specifics while preserving system responsibilities.

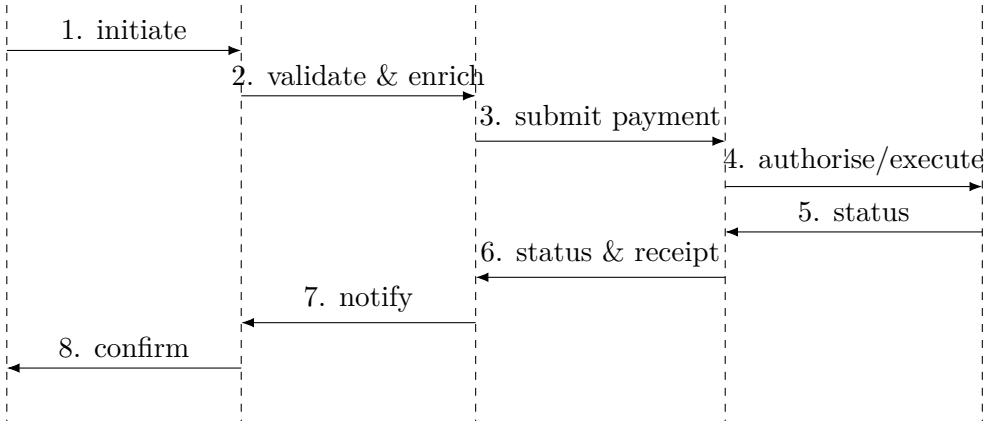

Figure 5.2: Conceptual online payment sequence (high-level).

5.3.2 Liquidity management and DCA mechanics

Liquidity management is a first-class domain: intermediaries require funding and defunding mechanisms to manage dedicated liquidity positions, commonly described as a Dedicated Cash Account (DCA). Industry guidance discusses DCA funding/defunding and limit mechanics, including "waterfall" and "reverse waterfall" flows (**eba_guide_2023**). In implementation, the DEIL should integrate with bank treasury systems and intraday liquidity monitoring.

5.3.3 Offline and synchronisation

Offline functionality adds additional state synchronisation and risk controls. The ECB cost note suggests the offline digital euro is expected to leverage online functionality to a large extent and that add-on cost may be limited, though precise procurement-based costs remain to be validated (**ecb_costs_2025**). From an integration standpoint, offline requires:

- device secure element management (card/phone secure enclave),

- risk parameters (offline limits, velocity controls),
- reconciliation and delayed settlement posting,
- dispute and double-spend detection mechanisms,
- incident and fraud handling workflows.

Algorithm 1 Offline payment synchronisation (conceptual)

1: **Input:** local offline transactions T_{local}, last sync token s
2: Verify device integrity and secure element counters
3: Create reconciliation batch $B \leftarrow \text{canonicalise}(T_{local}, s)$
4: Sign batch: $\sigma \leftarrow \text{Sign}_{HSM/SE}(B)$
5: Submit (B, σ) to Access Gateway via DEIL
6: Receive result set R (accepted/rejected, updated counters, new sync token s')
7: Apply outcomes: mark accepted txns settled; quarantine rejected for review
8: Update local state with s' and refreshed limits

Chapter 6

Affected bank/PSP components

6.1 Impact map

Table **??** lists key bank modules impacted by digital euro integration, aligned with the PwC "payment layer model" decomposition and Eurosystem domain framing (**pwc_coststudy_2025**; **ecb_rdg_progress_2025**).

Table 6.1: Impacted bank/PSP components and primary integration responsibilities

Module	**Change impact**	**Primary domain(s)**
Customer channels (mobile/web)	Digital euro wallet UI/UX, payment initiation, transaction history, notifications, customer support hooks.	Access, Transaction
Cards / secure elements	Optional physical form factor, SE provisioning, lifecycle mgmt, offline limits.	Access, Offline
POS / e-commerce acceptance	Terminal upgrades, QR/NFC flows, payment pages, merchant onboarding, acquiring alignment.	Transaction, Reference data
Branch & ATM network	Onboarding/offboarding support, funding/defunding services, cash-like accessibility.	Access, Liquidity
Payments hub / orchestration	New rail routing, state machine, idempotency, retries, reconciliation, disputes primitives.	Transaction
Core banking / accounts	Customer account linking (if applicable), statements, accounting postings, GL, fees.	Transaction, Reporting
Treasury / liquidity	DCA funding/defunding, intraday liquidity, limits, monitoring.	Liquidity
Risk, fraud, AML/CFT	KYC alignment, transaction monitoring, sanctions screening, fraud controls.	Access, Transaction
Data & reporting	Regulatory reporting, audit trails, operational metrics, incident reporting.	Reporting
Integration & security	Gateway adapter, key mgmt, signing, API version mgmt, certification/testing.	Cross-cutting

6.2 Interfaces and integration glue

The DEIL should be implemented as a bounded context that isolates the rest of the bank from scheme evolution. It typically exposes two northbound interfaces:

- **Channel APIs**: SDKs for mobile/web; device provisioning for offline.
- **Bank internal integration**: event streams and synchronous calls to payments hub, treasury, AML, CRM.

Southbound, it hosts adapters for access gateway REST/gRPC and related security requirements (**ecb_innovation_annex_2025**).

6.3 Operational processes impacted

Beyond technology, banks must adjust processes:

- customer onboarding/offboarding and customer support,
- incident management and fraud operations,
- change management and certification against scheme conformance tests,
- vendor management and outsourcing controls (DORA-aligned),
- business continuity and cyber-resilience exercises.

The operational layer (fee calculation, reporting/payment statistics, processes) is explicitly represented as part of overall cost and effort in industry studies (**pwc_coststudy_2025**).

Chapter 7

Shared vs. dedicated integration components

7.1 Rationale for mutualisation

The ECB cost analysis emphasises that banks already make extensive use of shared solutions for payment channels, accounts, compliance, and operational support, and argues that digital euro integration can similarly leverage shared infrastructures (**ecb_costs_2025**). It further quantifies that cost mutualisation can materially reduce total investment costs and that banks would not have to implement on a stand-alone basis (**ecb_costs_2025**).

7.2 Taxonomy of mutualisable components

Table **??** classifies components by mutualisation potential, including software and hardware/physical infrastructure dimensions.

Table 7.1: Shared vs. dedicated components: candidate mutualisation scope

Component	Why it can be shared	Typical host
Access gateway adapter (REST/gRPC, signing, versioning)	Standardised protocol and security patterns; economies of scale in certification and upgrades.	Vendor / utility / group IT
Conformance testing harness & sandbox tooling	High fixed cost; reusable across participants; reduces duplicated effort.	Utility / consortium
Offline device lifecycle services (SE provisioning, key injection)	Hardware security requires specialised tooling; shared HSM/PKI can reduce cost.	Utility + HSM provider
Acceptance utilities (POS/ATM upgrade programs)	Merchants/ATMs often served by shared utilities; aligns with replacement cycles and outsourcing trends.	Acquirer/ATM utility
Shared fraud signal exchange (optional)	Cross-bank fraud patterns; shared analytics platform can improve detection.	Consortium
Reference data distribution (scheme reference data, alias portability adapters)	Standard data sets and portability workflows benefit from central services.	Utility
Bank customer relationship data	Differentiation and privacy constraints; bank-specific.	Bank
Bank-specific risk appetite & AML rules	Local regulation, internal policies and models differ.	Bank
Treasury strategy and intraday liquidity	Balance sheet and liquidity policies differ.	Bank

7.3 Hardware/physical mutualisation: POS and ATM

Industry cost evidence shows that acceptance infrastructure and ATM/branch networks are major cost drivers (**pwc_coststudy_2025**). The ECB cost note adjusts ATM upgrade assumptions partly due to the trend toward outsourcing ATMs to independent deployers and utilities and due to existing NFC/QR-enabled ATM footprints, discounting ATM upgrade costs accordingly (**ecb_costs_2025**). This supports the thesis position that hardware upgrades can be mutualised via utilities and coordinated procurement, rather than executed separately by each bank.

Chapter 8

Implementation models

8.1 Model definitions

8.1.1 In-house

The bank builds and operates most of the DEIL and surrounding components, including gateway adapter, orchestration, data and reporting, and often custom channel experiences. It typically uses internal platform engineering capabilities (CI/CD, observability, SRE) and aims for strategic reuse across future payment initiatives.

8.1.2 Outsourced

The bank procures digital-euro-specific capabilities from a specialised provider (or banking group utility), integrating via a thin layer. Outsourcing is consistent with the ECB's focus on external synergies and cost mutualisation (e.g., "outsourcing to central providers or vendors") (**ecb_costs_2025**).

8.1.3 Hybrid

The bank keeps differentiating elements (customer channels, risk controls, CRM) while outsourcing commoditised or high-fixed-cost capabilities (gateway adapter, offline provisioning, conformance tooling). Hybrid is often the most practical model, aligning to cost mutualisation and bank-specific differentiation needs.

8.2 Architectural patterns

8.2.1 Modular monolith vs. microservices

- **Modular monolith**: faster delivery, simpler operations, strong consistency for payment state machines; risk of scaling bottlenecks if poorly modularised.

- **Microservices/event-driven**: better scalability and independent release cycles; higher operational complexity; requires mature DevSecOps and observability.

Given the criticality of payment flows, many banks adopt a hybrid: a payments state machine service (high integrity) plus event-driven integration to AML, notifications, reporting.

8.2.2 Integration styles

- **API-first synchronous**: suitable for real-time authorisation, channel UX.
- **Event-driven**: suitable for monitoring, reconciliation, reporting, fraud signals.
- **Batch**: used for end-of-day settlement accounting and regulatory reporting extracts.

8.3 Bank-tier-specific implementation strategy

8.3.1 Decision matrix

Table **??** maps recommended implementation models to bank tiers.

Table 8.1: Recommended implementation model by bank tier (baseline)

Tier	**Typical profile**	**Recommended model**	**Rationale**
Tier 1	Complex channels, strong engineering, high transaction volumes	In-house or Hybrid	Strategic control, scale benefits, reuse; still outsource commoditised components for efficiency.
Tier 2	Large banks with sizeable channels and constraints	Hybrid	Balance between differentiation and cost mutualisation; focus on reuse and shared gateway/offline services.
Tier 3	Mid-sized banks, limited platform engineering	Hybrid leaning outsourced	Adopt shared gateway adapter and offline provisioning; keep AML/risk integration in-house.
Tier 4	Small banks/LSIs	Outsourced / utility model	Minimise fixed costs; rely on shared providers and central apps where permitted; focus on compliance and customer servicing.

8.3.2 MCDA scoring example

Table **??** provides an illustrative MCDA. Scores are indicative and should be calibrated with institution-specific parameters.

Table 8.2: Illustrative MCDA criteria and weights

Criterion	Weight	Notes
Time-to-market	0.15	Faster delivery reduces regulatory/project risk.
CapEx (build)	0.15	Up-front build costs; impacted by channel footprint.
OpEx (run)	0.10	Operational burden and SRE staffing.
Integration risk	0.15	Coupling to core systems and maturity of APIs.
Security/compliance fit	0.15	AML/KYC, auditability, privacy requirements.
Operational resilience	0.15	High availability, cyber resilience (DORA-aligned).
Vendor lock-in risk	0.10	Exit cost and concentration risk.
Reuse potential	0.05	Leverage for future payment innovations.

Chapter 9

Cost and resource analysis

9.1 Public cost estimates

The PwC industry study estimates introduction costs exceeding 2 billion for 19 participating banks (excluding offline, multiple accounts, merchant acquiring), with an average of 110 million per bank, and extrapolates total euro-area change costs to 18 billion (**pwc_coststudy_2025**). It reports that technical adjustments account for around 75% of costs and that respondents expect roughly 46% of relevant skilled resources to be tied up per year (**pwc_coststudy_2025**).

The ECB cost note, accounting for synergies and cost mutualisation, suggests total costs could lie within 4–5.77 billion over four years (1–1.44 billion annually) and references a European Commission impact assessment range of 2.8–5.4 billion (**ecb_costs_2025**). The ECB analysis emphasises that banks need not implement on a stand-alone basis and that external synergies (shared providers/vendors) are key (**ecb_costs_2025**).

9.2 Tier-based cost table

The ECB cost note summarises PwC size-cluster estimates (four-year totals) of approximately 182 million for >1 trillion banks, 106 million for 100b–1tr banks, 29 million for 30b–100b banks, and 9 million for <30b banks (**ecb_costs_2025**). These numbers provide a useful baseline for tier modelling.

Table 9.1: Indicative four-year investment cost per bank (PwC cluster estimates as reported in ECB cost note)

Bank size cluster	Cost per bank (m)
> 1 trillion	182
100b – 1tr	106
30b – 100b	29
< 30b	9

9.3 Synergy scenarios

The ECB cost note models group synergies (e.g., within IPS or shared IT providers) ranging from 90–98% in the base scenario, and market synergy factors around 30% (weighted), with alternative low and high synergy scenarios (**ecb_costs_2025**). These synergy factors operationalise the potential value of shared integration services and underpin the thesis recommendation to prioritise mutualisable components.

9.3.1 Illustrative chart

Figure **??** visualises the headline range of total euro-area cost estimates from published studies and synergy-adjusted ECB analysis.

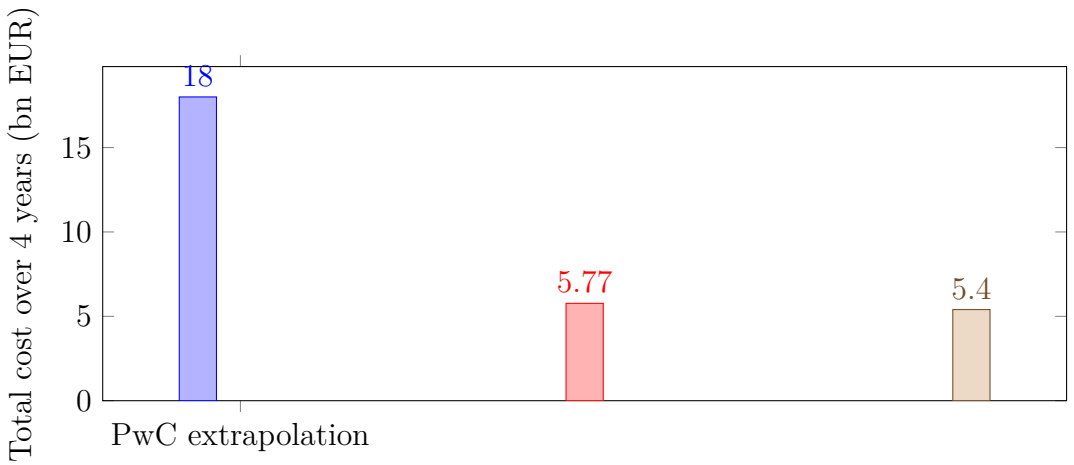

Figure 9.1: Indicative total cost comparisons (upper bounds shown for ranges). Sources: **pwc_coststudy_2025<empty citation>** and **ecb_costs_2025<empty citation>**.

9.4 IT spending context and capacity constraints

Sector survey data for the Italian banking sector reports substantial aggregate ICT costs and a significant share of third-party spending, suggesting material reliance on external providers and supporting the plausibility of utility/shared-service models for new regulatory initiatives (**cipa_rilevazione_it_2025**). The PwC study further highlights resource capacity constraints (skilled personnel share) as a key risk (**pwc_coststudy_2025**).

Chapter 10

Blueprints for bank-tier implementations

This chapter provides concrete blueprints for the three implementation models and highlights module placement decisions.

10.1 Blueprint A: Tier 1–2 hybrid platform

10.1.1 Key characteristics

- Bank-operated DEIL on internal Kubernetes platform.
- Shared gateway adapter and conformance harness procured from a vendor (or built once at group level).
- Event-driven integration to AML/fraud and reporting; strict state machine service for payments.
- Dedicated offline device management service shared across subsidiaries.

10.1.2 Component placement

Table 10.1: Tier 1–2 hybrid blueprint: component ownership

Component	Description	Owner
DEIL orchestration	Payment state machine, idempotency, retries, reconciliation	Bank
Gateway adapter	REST/gRPC client, signing, version mgmt, certification	Shared vendor/utility
AML/fraud connectors	Screening, monitoring, case management integration	Bank
Offline provisioning	SE lifecycle, key mgmt, counters, risk params	Shared (group/utility)
Channel UX	Wallet UI, merchant flows, notifications	Bank

10.2 Blueprint B: Tier 3 hybrid-leaning-outsourced

Mid-sized banks typically benefit from utility services for gateway adapter, offline and acceptance upgrades. Banks retain compliance/risk integration due to local policy requirements.

10.3 Blueprint C: Tier 4 outsourced/utility model

Tier 4 banks minimise fixed costs by:

- Consuming a hosted DEIL service (multi-tenant) plus shared gateway adapter.
- Using centrally provided channel components where permitted (e.g., standard wallet UI) and integrating only customer servicing and compliance hooks.
- Relying on merchant/acquirer utilities for acceptance upgrades and on ATM utilities for physical access paths.

This aligns with ECB emphasis that banks need not implement the digital euro on a stand-alone basis and can rely on shared solutions (**ecb_costs_2025**).

Chapter 11

Governance, risk, and compliance considerations

11.1 Regulatory alignment

Legislative discussions emphasise that the digital euro would complement cash and provide payment functionality across the euro area (**eu_council_2025_digital_euro_position**). Banks must implement in a way consistent with scheme rules and supervisory expectations around operational resilience.

11.2 Operational resilience and DORA

Digital euro integration extends the bank's critical payment perimeter. Key controls include:

- resilience-by-design (redundancy, failover, chaos testing),
- third-party risk management (vendor due diligence, concentration risk),
- incident response and reporting workflows,
- secure SDLC and cryptographic key governance.

11.3 Privacy and data protection

While privacy design is partly scheme-defined, intermediaries control significant data surfaces: customer identity, transaction monitoring, and support logs. Architecture should implement data minimisation, strong access controls, and auditable processing consistent with GDPR principles.

Chapter 12

Discussion

12.1 Answering the research questions

RQ1 is addressed via the DEIL-based reference architecture and integration patterns. **RQ2** is addressed via scheme vs intermediary responsibility mapping. **RQ3** is addressed through the component impact map and domain decomposition. **RQ4** is addressed through the mutualisation taxonomy, emphasising shared gateway/offline/acceptance utilities. **RQ5** is addressed through tiering, MCDA and blueprint recommendations.

12.2 Limitations

Rulebook details and technical specifications may evolve; therefore the architecture is designed to isolate scheme evolution behind adapters and versioning boundaries (**ecb_rdg_progress_2025**). Cost estimates remain sensitive to design choices (offline scope, multiple accounts, acquiring).

12.3 Future research

Future work could: (i) validate the blueprint using empirical case studies with banks/PSPs, (ii) extend cost modelling with institution-specific parameters, (iii) evaluate interoperability reuse for private payment schemes.

Chapter 13

Conclusion

This thesis provides a rulebook-aligned reference architecture and a pragmatic operating-model framework for banks integrating the digital euro. Evidence suggests that while stand-alone implementations could be costly, significant cost mutualisation is feasible through shared services and utilities (**ecb_costs_2025**). The recommended approach is tiered: large banks adopt hybrid/in-house architectures for strategic control and reuse, while smaller institutions leverage outsourced/utility models to reduce fixed costs and operational burden. Across all tiers, careful modularisation of gateway adapters, offline services, and acceptance infrastructure enables interoperability, resilience, and the potential to reuse digital euro standards for broader European payment innovation.

Appendix A

Appendix: PwC layer distribution chart

Figure **??** shows an illustrative representation of the PwC reported cost-layer distribution (commercial/technical/operational).

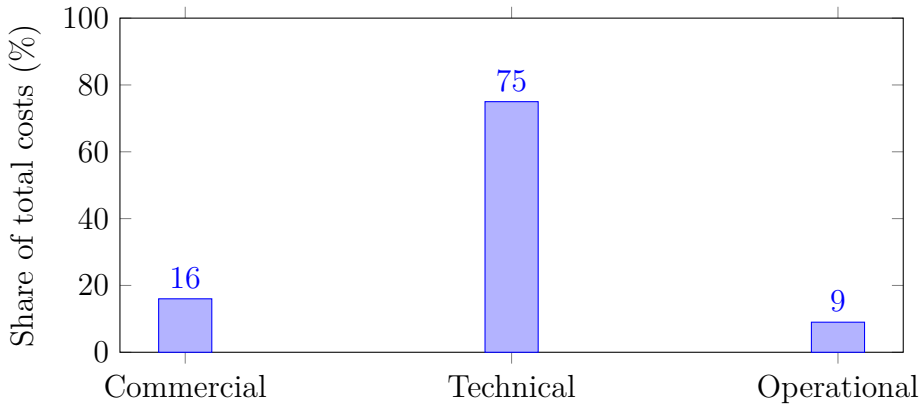

Figure A.1: Cost distribution across PwC payment layer model (reported shares). Source: **pwc_coststudy_2025<empty citation>**.

Appendix B

Appendix: Practical checklist for banks

1. Establish target operating model (in-house/hybrid/outsourced) and vendor strategy.
2. Build domain-aligned backlog: access, transaction, liquidity, offline, reporting.
3. Stand up DEIL boundary: API gateways, signing, versioning, test harness.
4. Integrate treasury/DCA processes and limit controls.
5. Integrate AML/fraud monitoring and customer support workflows.
6. Plan acceptance upgrades (POS/ATM) with utilities; align with replacement cycles.
7. Execute conformance testing and operational readiness (BCP, incident response).