Statement on the Digital Euro

Frequently Asked Questions Revisited

Özgür Kesim[1], Mikolai Gütschow[2]

2026-06-05

[1]) Code Blau GmbH & FU Berlin [2]) TU Dresden

oec@taler.net

The digital euro:

A CBDC for the Euro zone

The digital euro:

A CBDC for the Euro zone

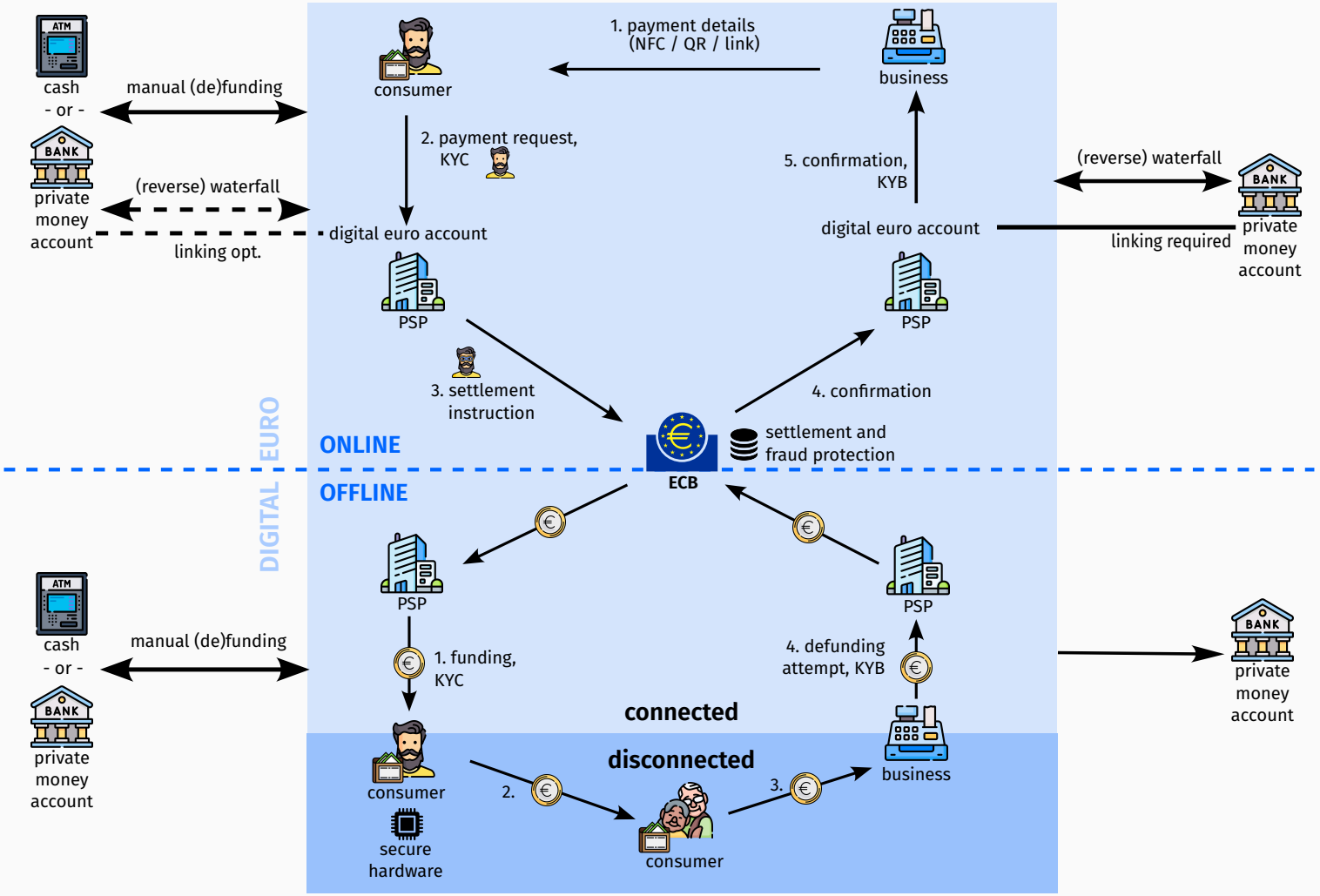
Sources: ECB progress reports 2021–2026, EP Legislative Train Schedule, European Commission COM/2023/369, Council of the EU, Dec 2025, ECB speech before ECON, 3 Jun 2026. As of June 2026.

Agenda

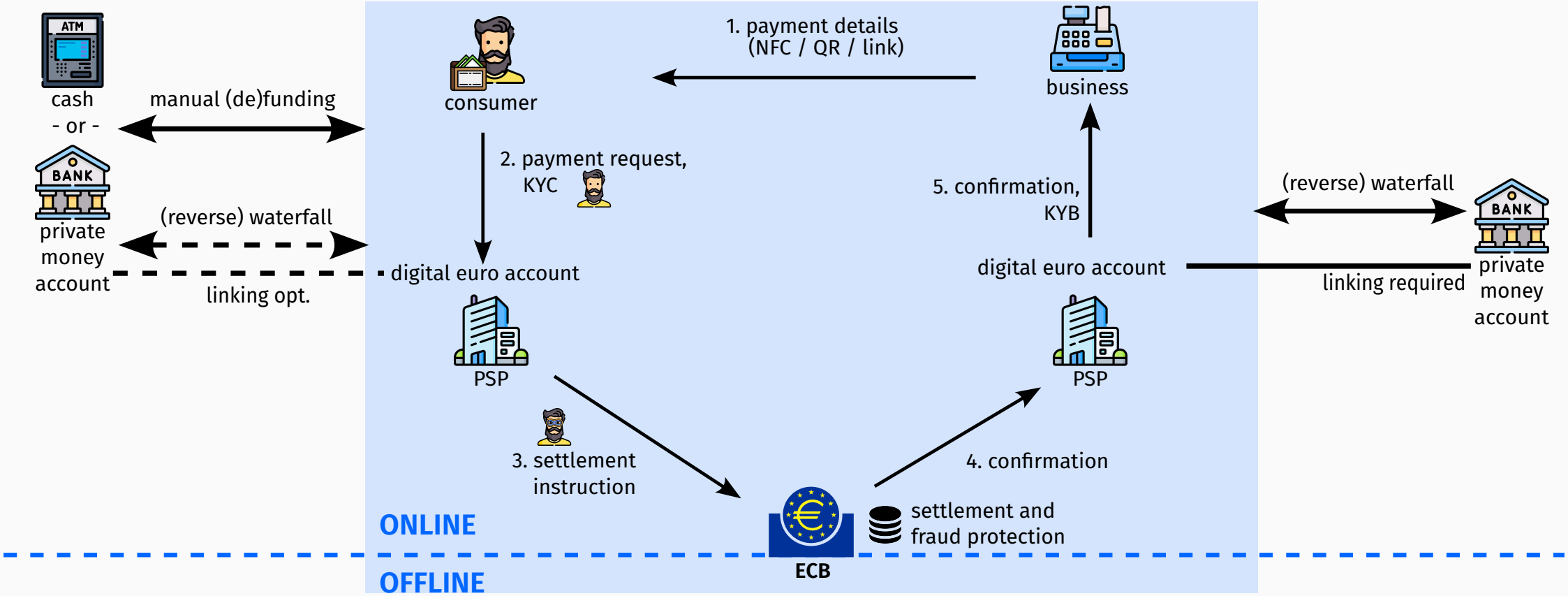
- We take a closer look
  at the “digital euro FAQ” [1] and other publications by the ECB [2],
- examine the design of the digital euro in terms of
  privacy, technical feasibility, risks, costs and utility,
- and discuss the key findings [3].

The Digital Euro Design

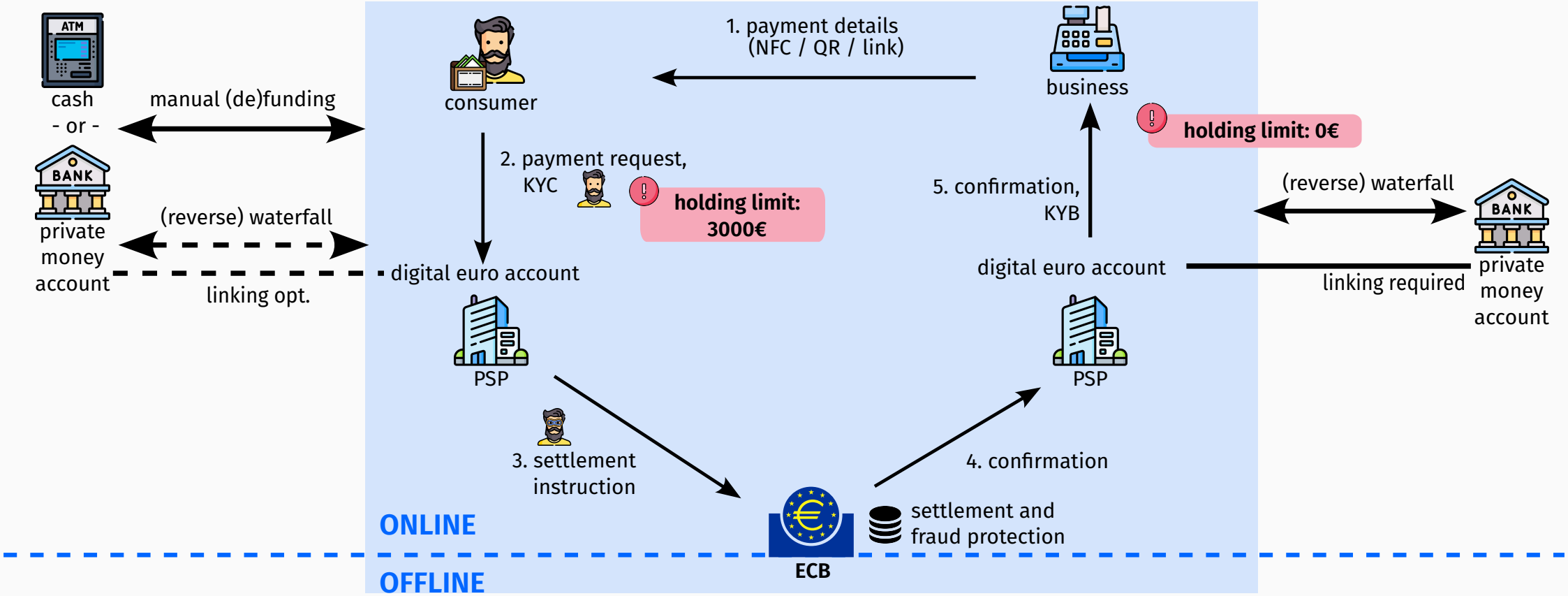
The Digital Euro Design



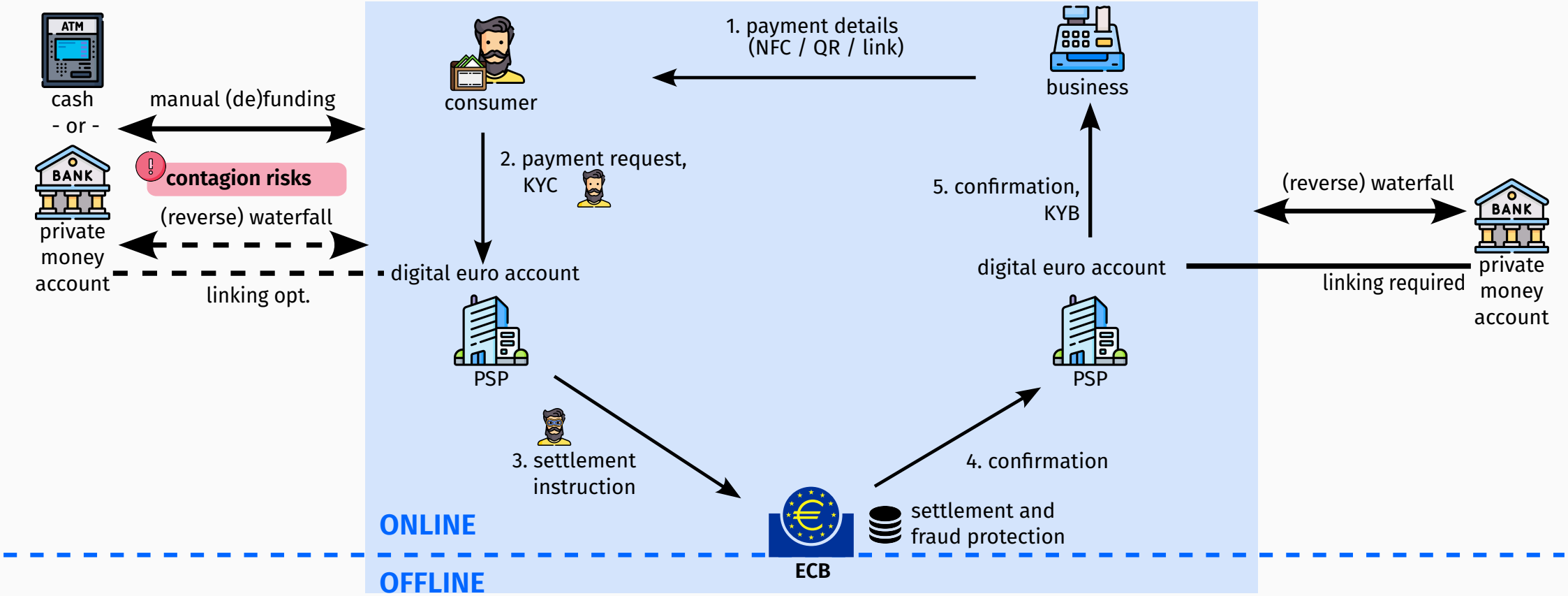
Online Overview



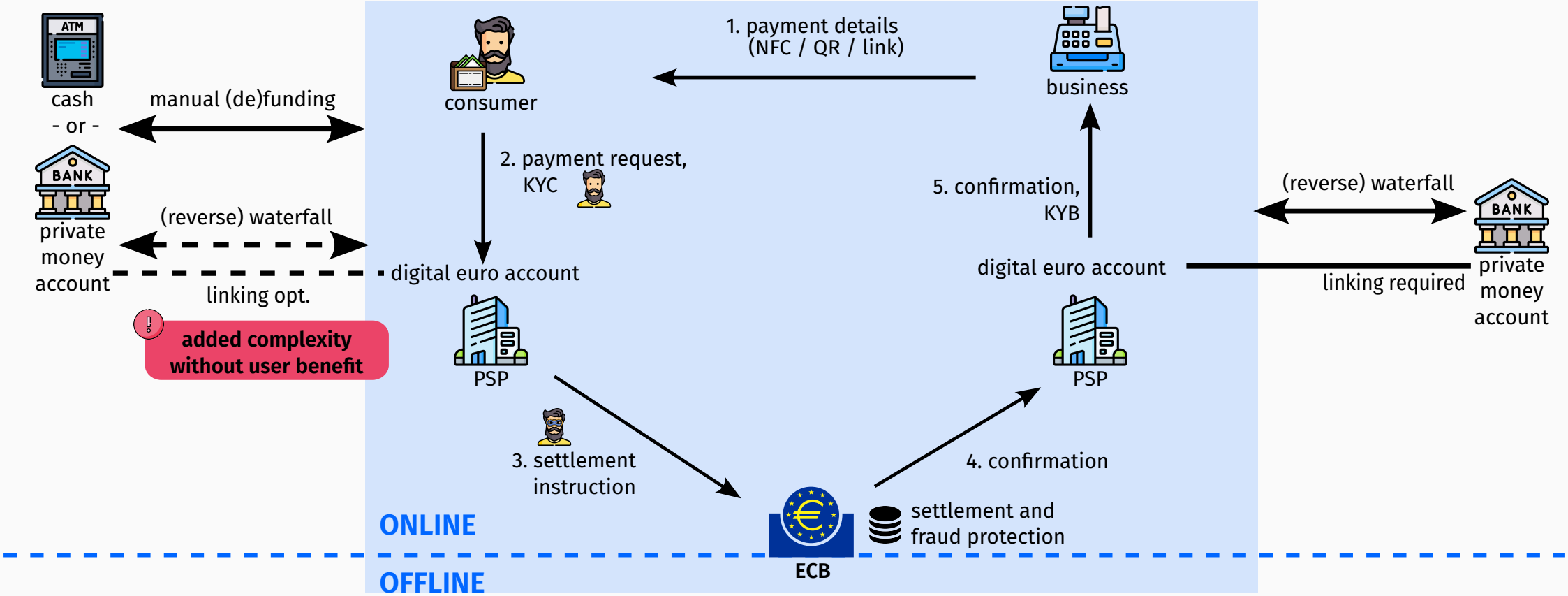
Online Problems - Holding limits



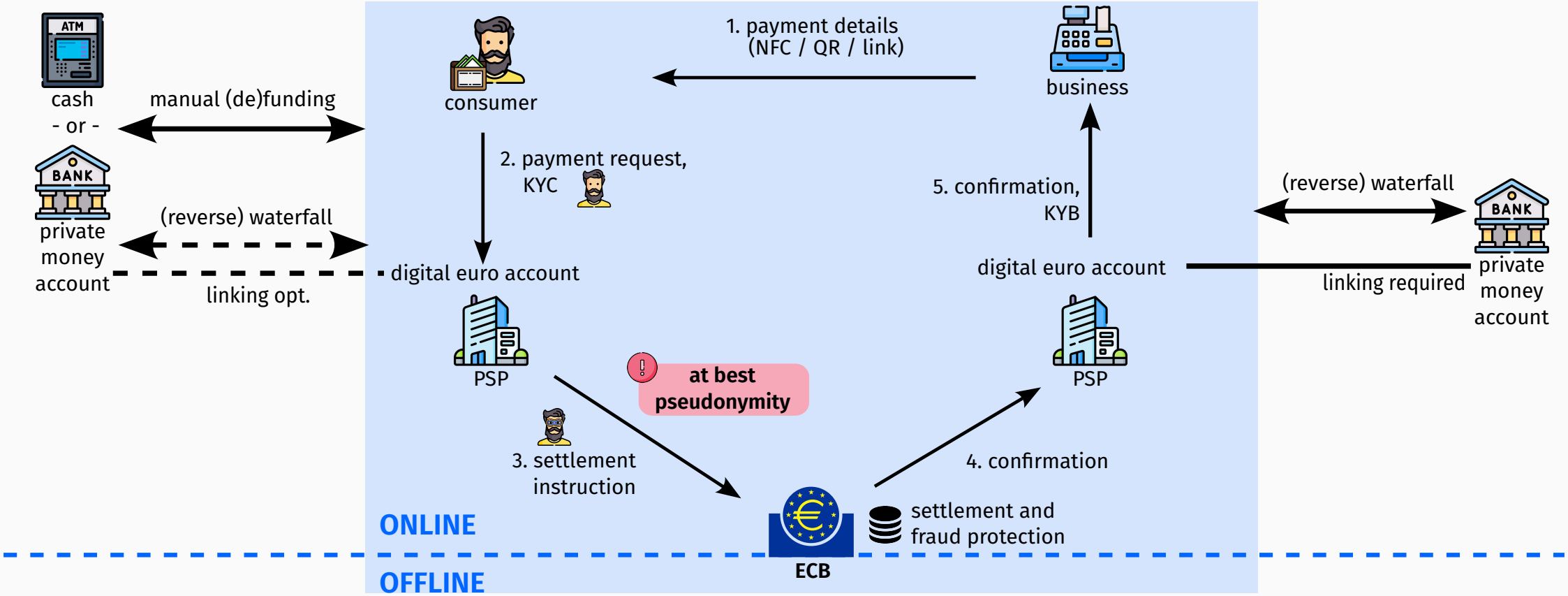
Online Problems - Contagion risk through reverse waterfall



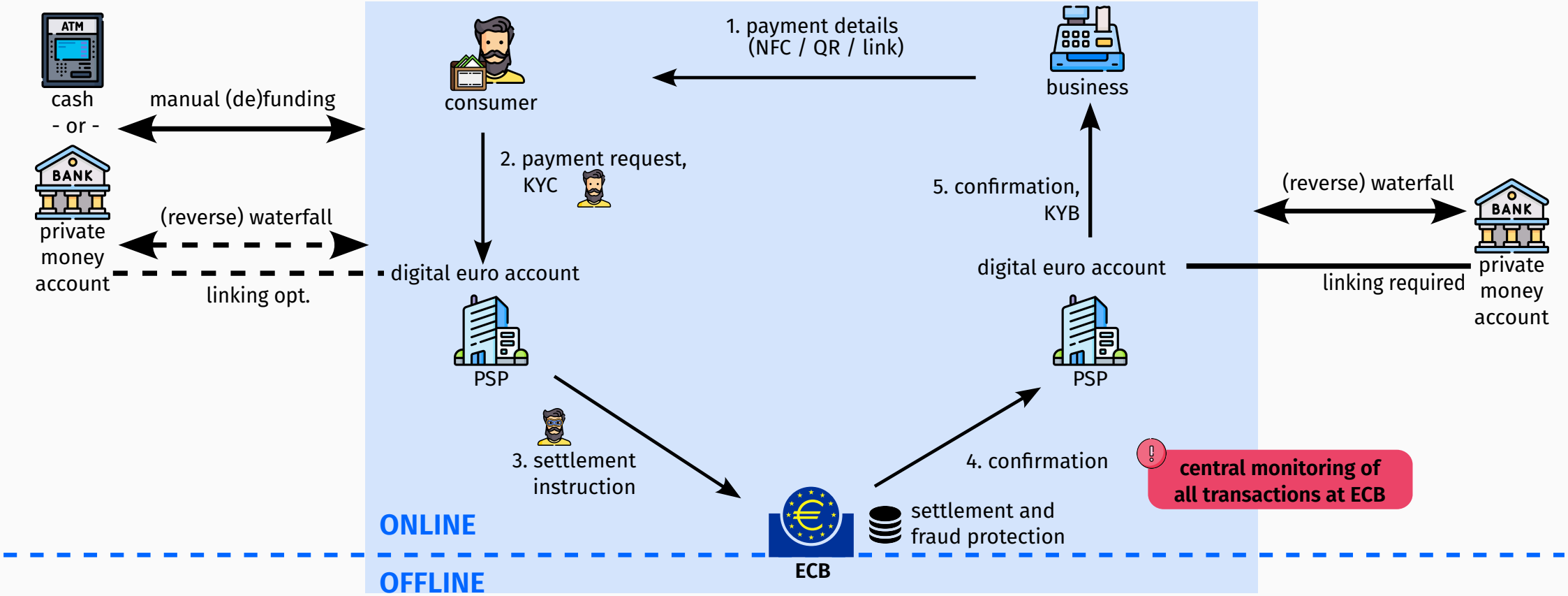
Online Problems - Complexity without benefit



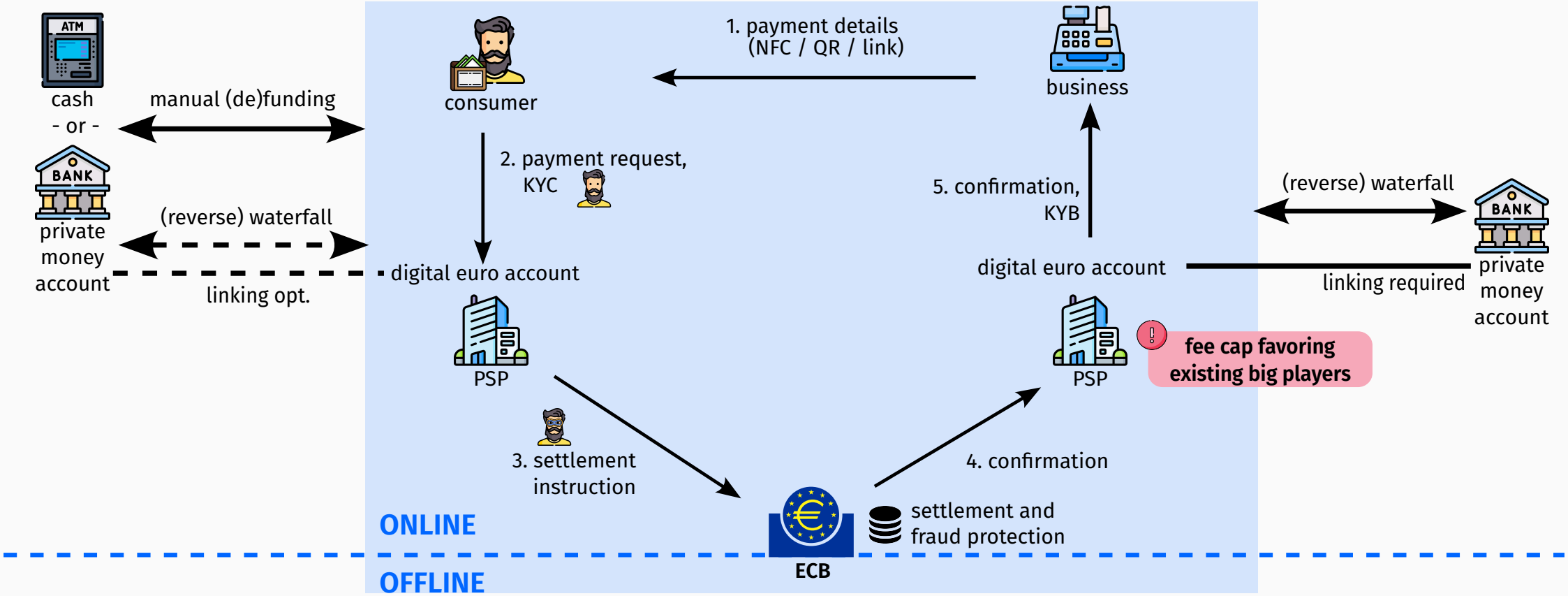
Online Problems - Only pseudonymity for users



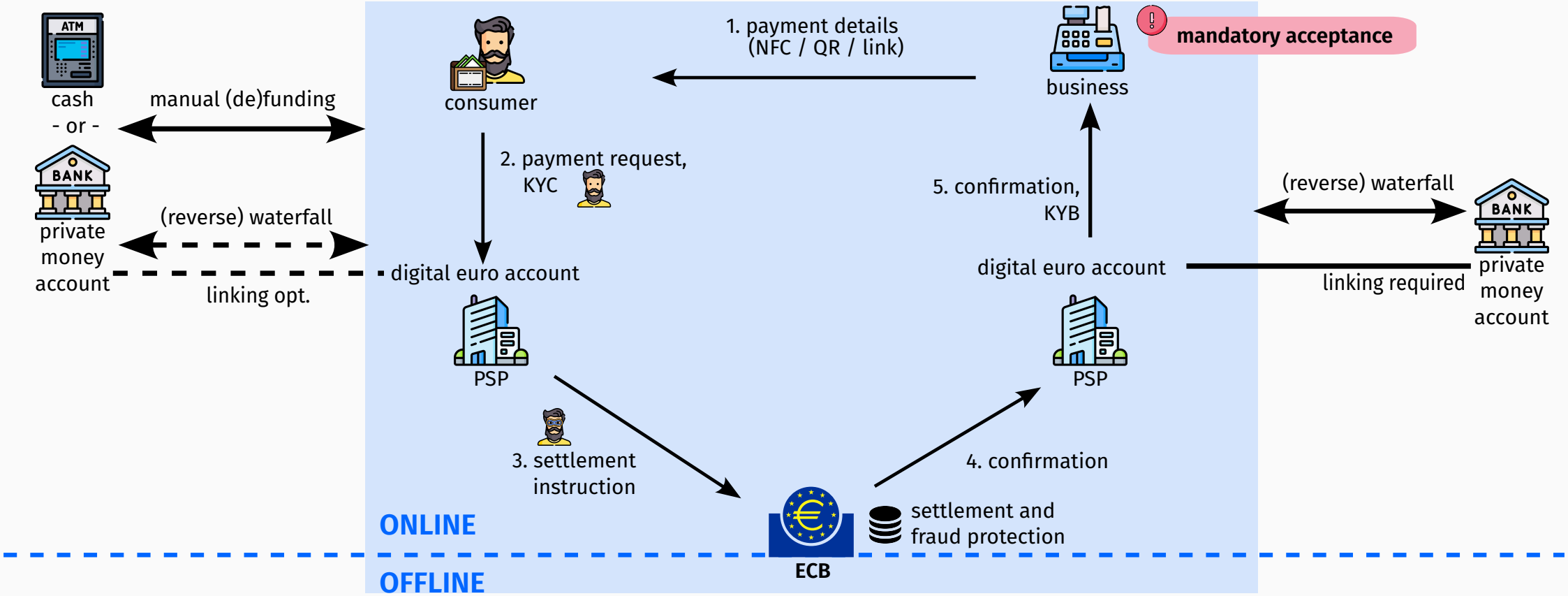
Online Problems - Central monitoring of all transactions



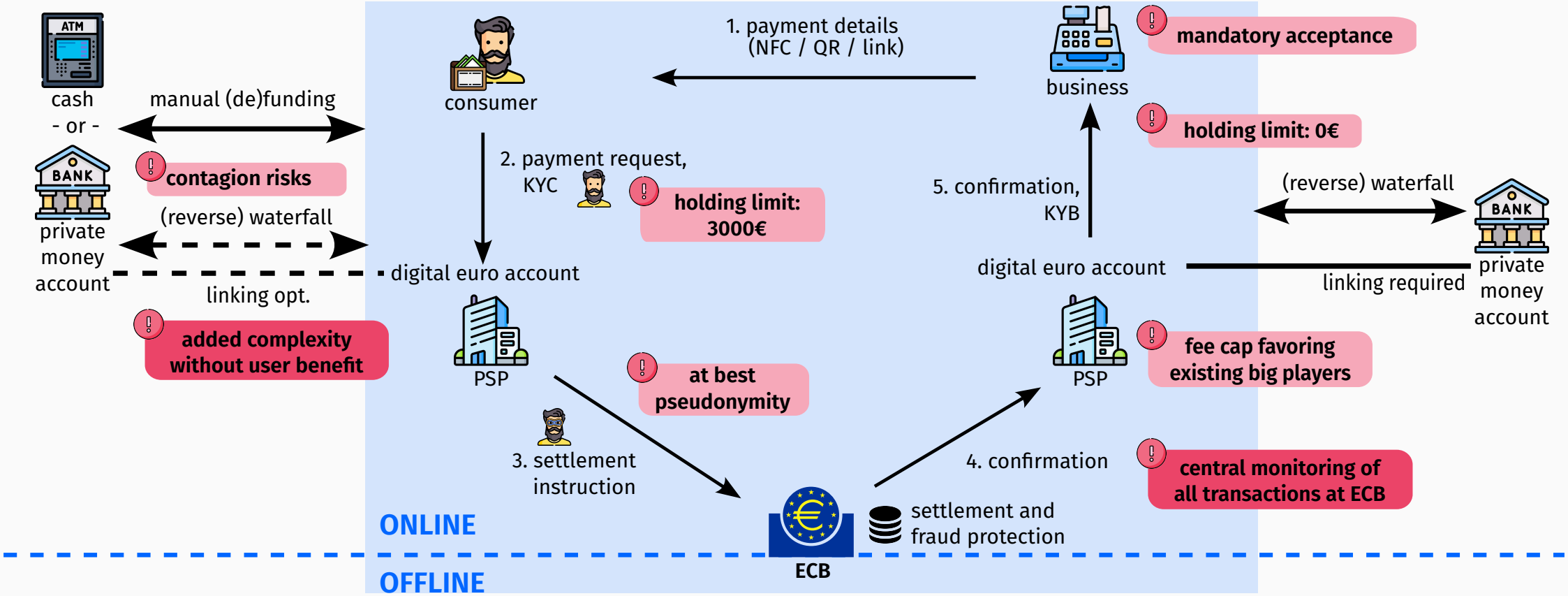
Online Problems - Fee cap desincentive



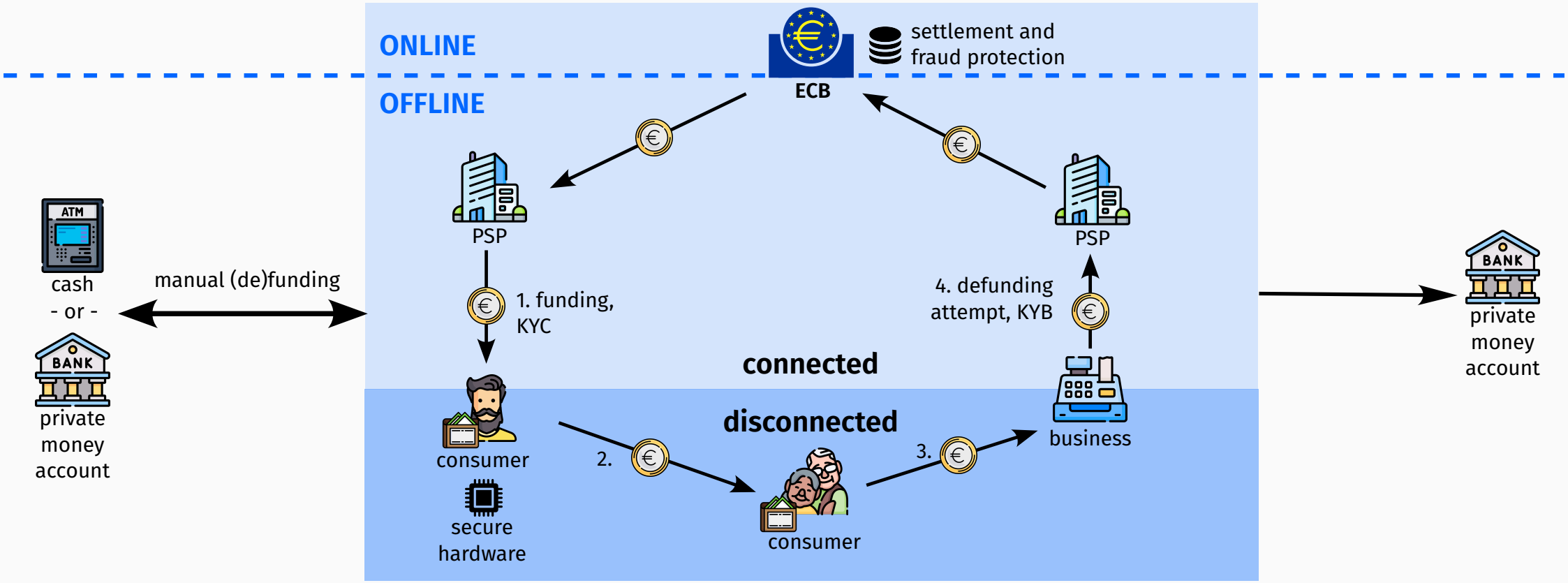
Online Problems - Mandatory acceptance



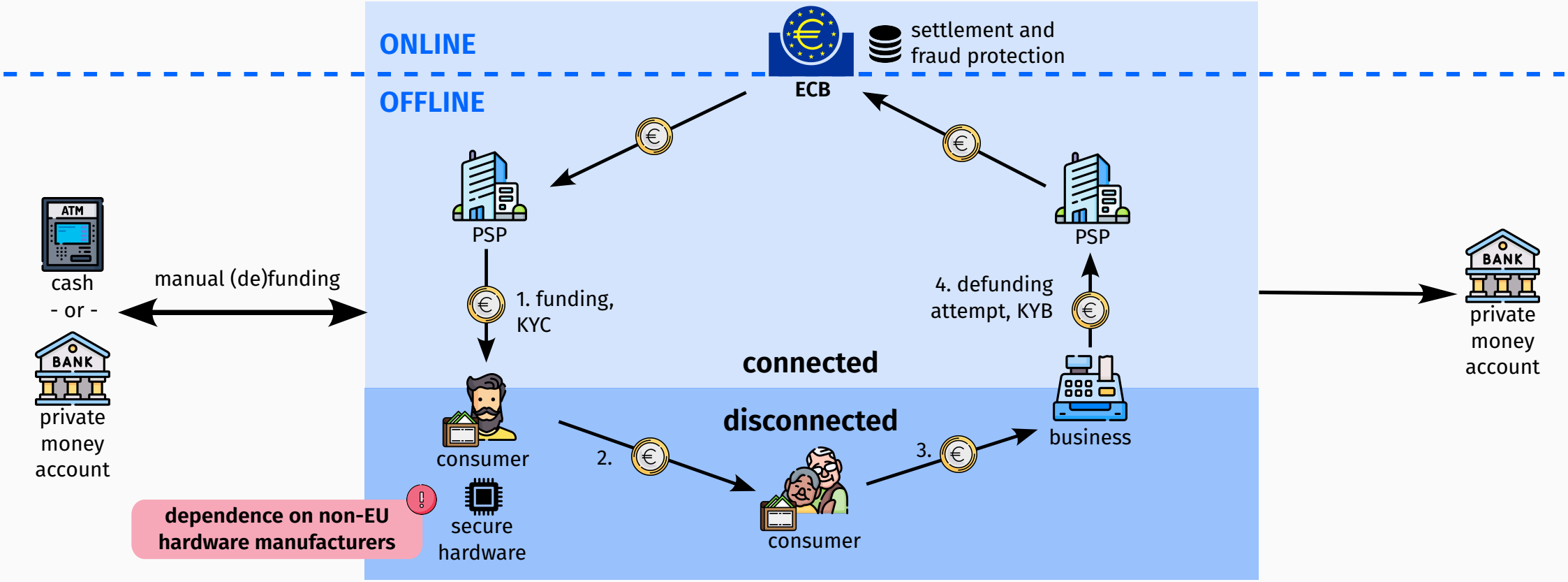
Online Problems



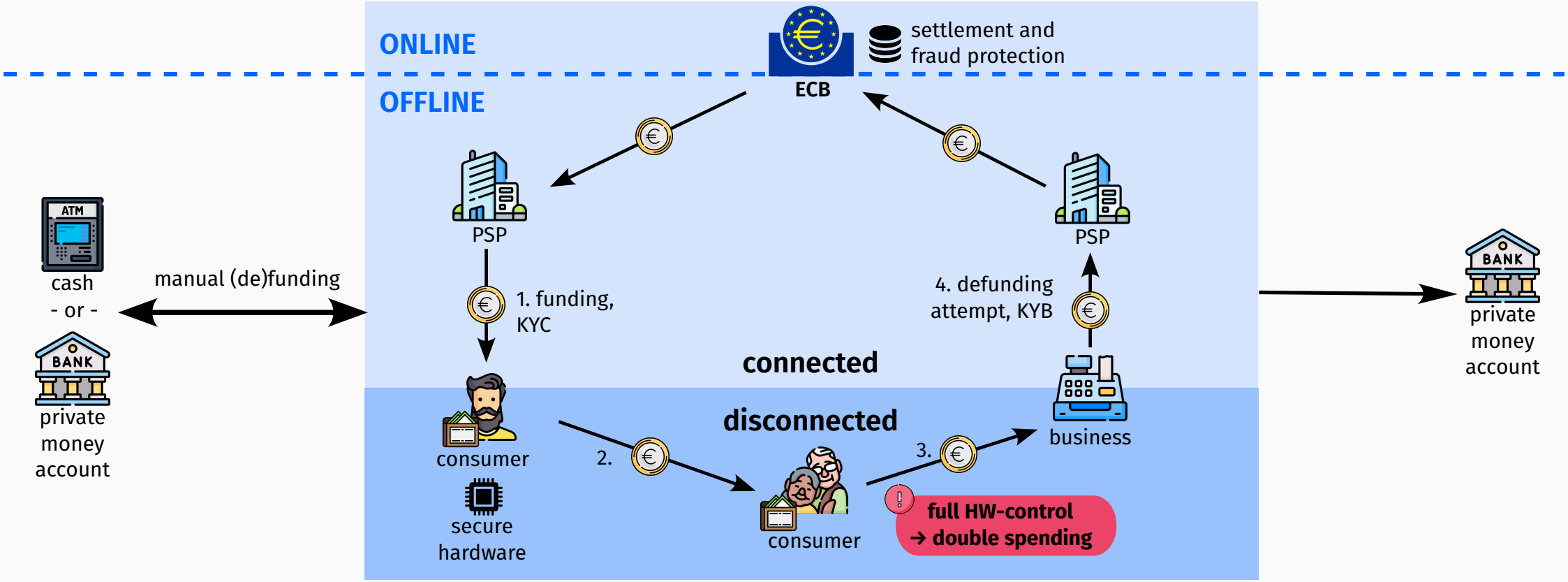
Offline Overview



Offline Problems - Dependence on non-EU HW-manufacturers



Offline Problems - User control of HW leads to double spending



CAP Theorem, Hardware Security and Double Spending

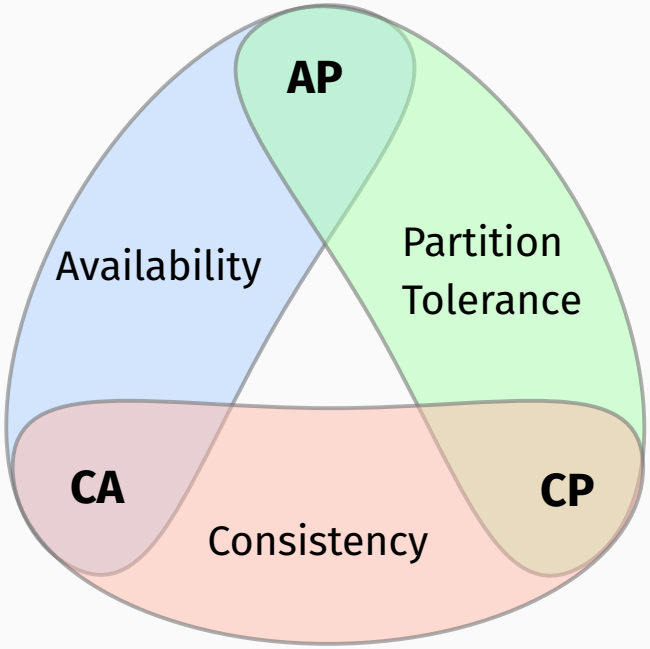
The CAP Theorem for distributed systems

The CAP Theorem [4] establishes:

No distributed system can be

- partition-tolerant,
- available,
- and consistent

at the same time.



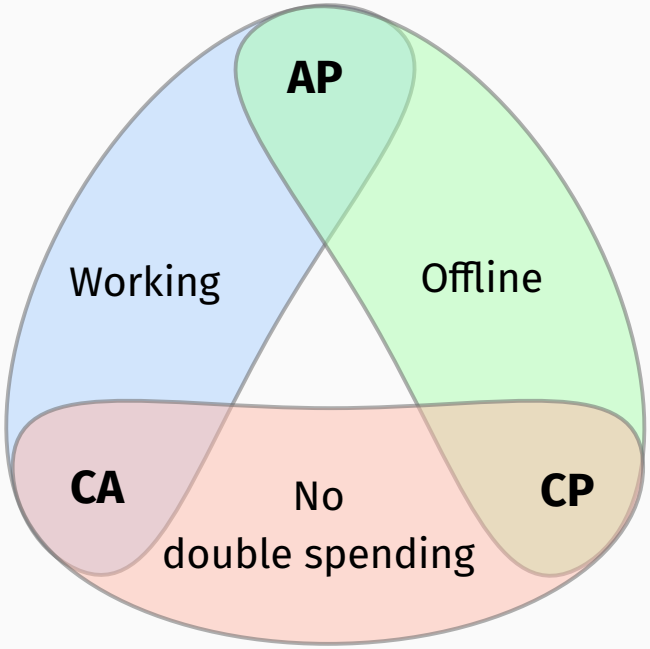
The CAP Theorem for payment systems

For payment systems that means:

No payment system can be

- **offline**,
- **still work**,
- and **without double spending**

at the same time.



Double Spending protection via Secure Hardware

According to the design for the digital euro,
secure hardware in the user's device
shall protect against double spending.

Essentially by enforcing consistency via a
protected environment in the (offline) device.

Purpose of Secure Hardware

User centric threat model:

Protect

- data of the user
- on its own device
- from malicious apps

Think: PIN, passwords, ...

Purpose of Secure Hardware

User centric threat model:

Protect
- data of the user
- on its own device
- from malicious apps

Think: PIN, passwords, ...

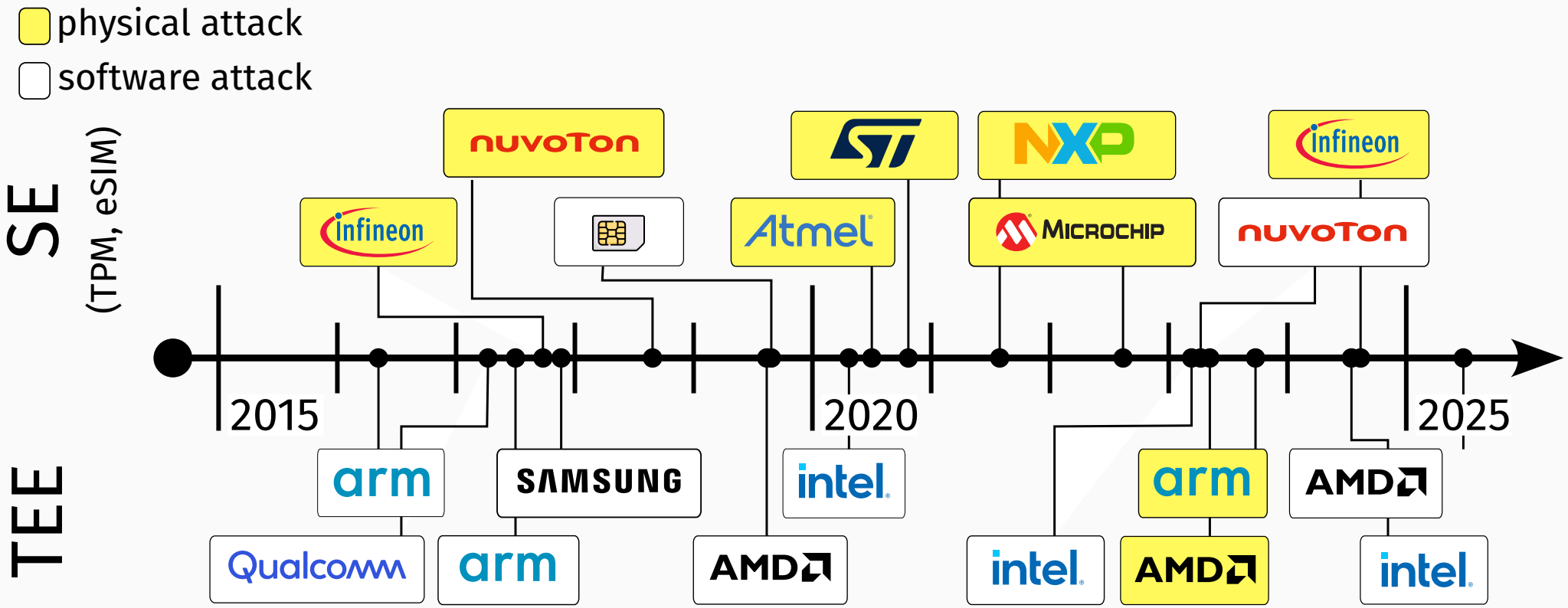
However, in the context of the digital euro, the **threat model is different**:

Protect
- data of the **ECB/PSP**
- on the **user's** device
- **from the user** (and malicous apps)

→ Users have monetary incentive to **break their own hardware**

Think: Playstation, DVD, ...

Hardware Security: History of Attacks



Sean Heelan's Blog

SOFTWARE EXPLOITATION AND OPTIMISATION

AI

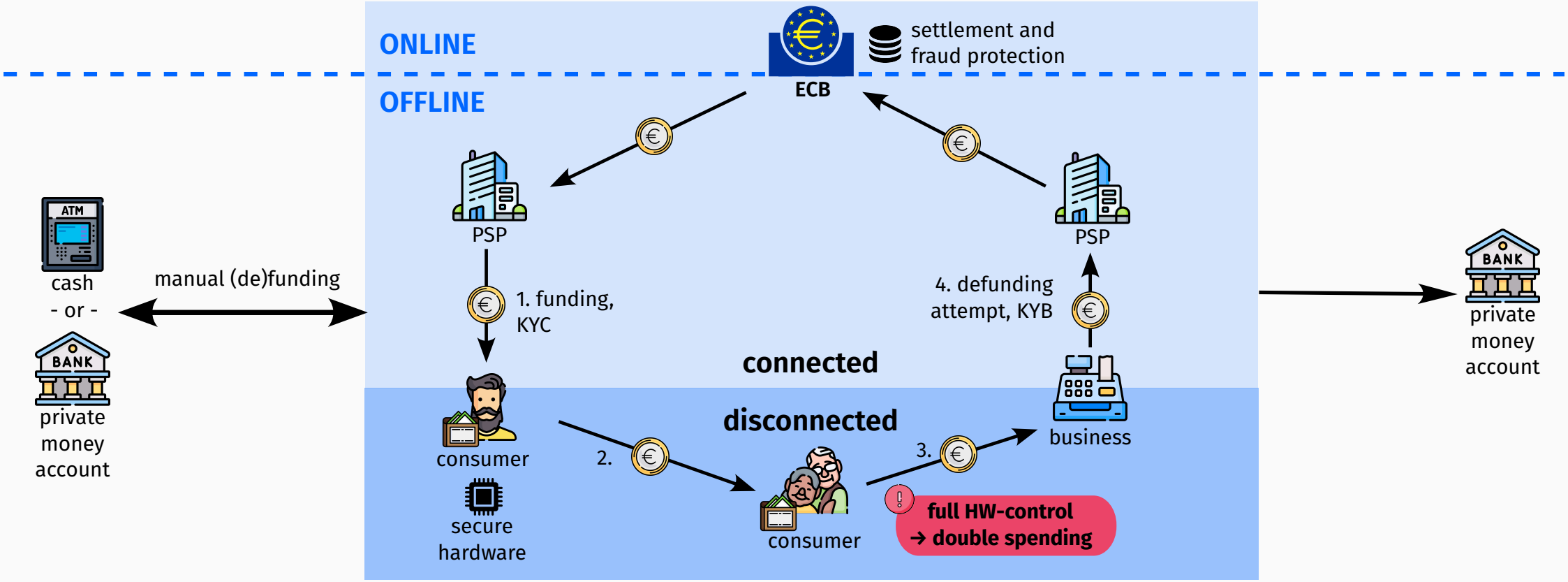
On the Coming Industrialisation of Exploit Generation with LLMs

JANUARY 18, 2026 SEANHN

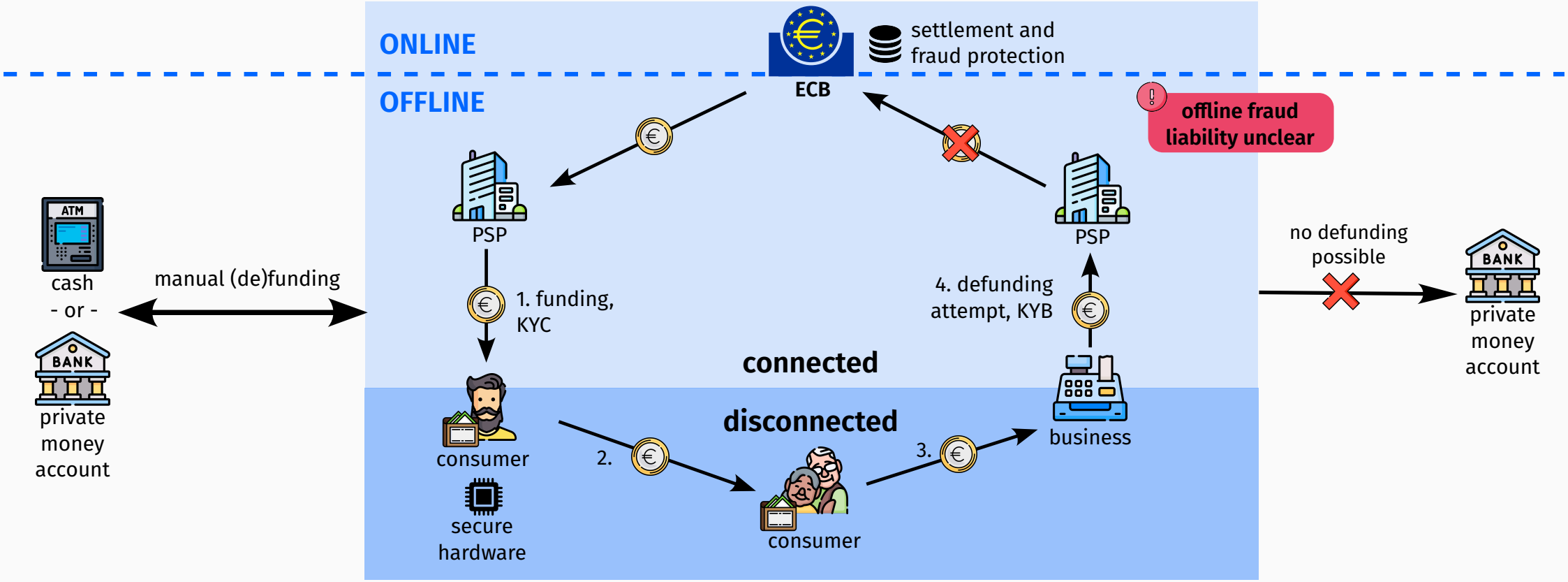
Follow @seanhn

Recently I ran an experiment where I built agents on top of Opus 4.5 and GPT-5.2 and then challenged them to write exploits for a zeroday vulnerability in the QuickJS Javascript interpreter. I added a variety of modern exploit mitigations, various constraints (like assuming an

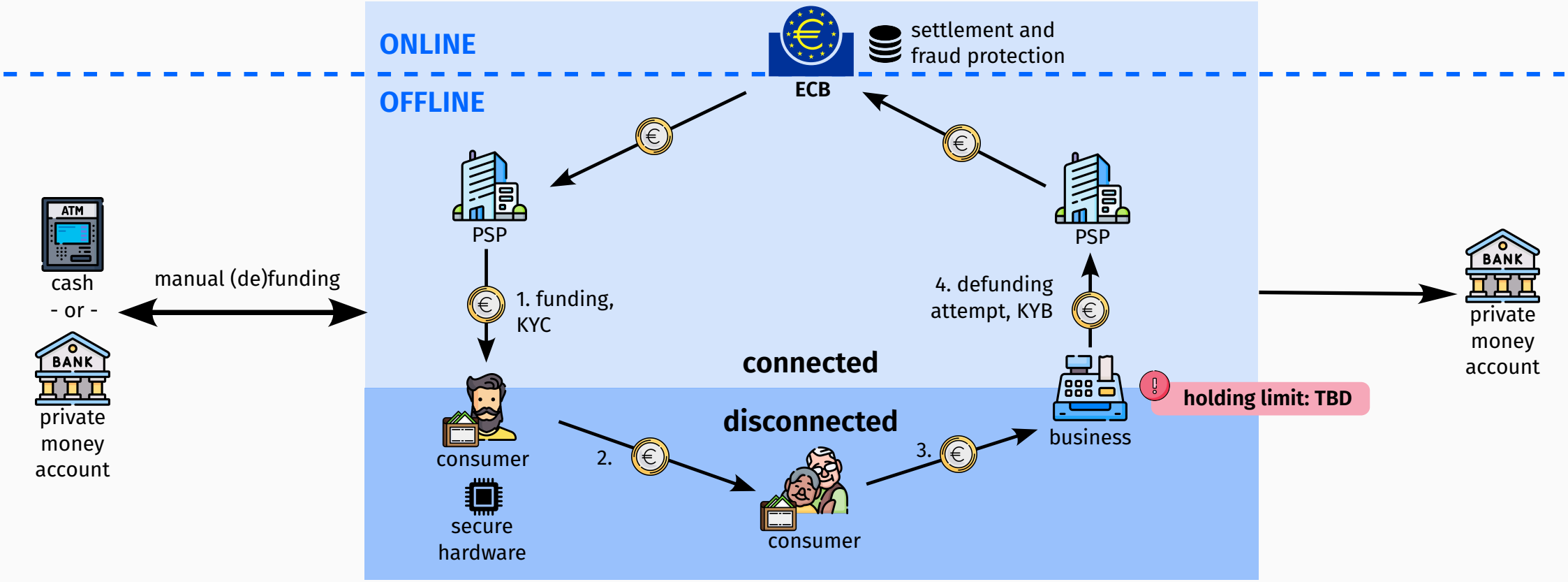
Offline Problems - User control of HW leads to double spending



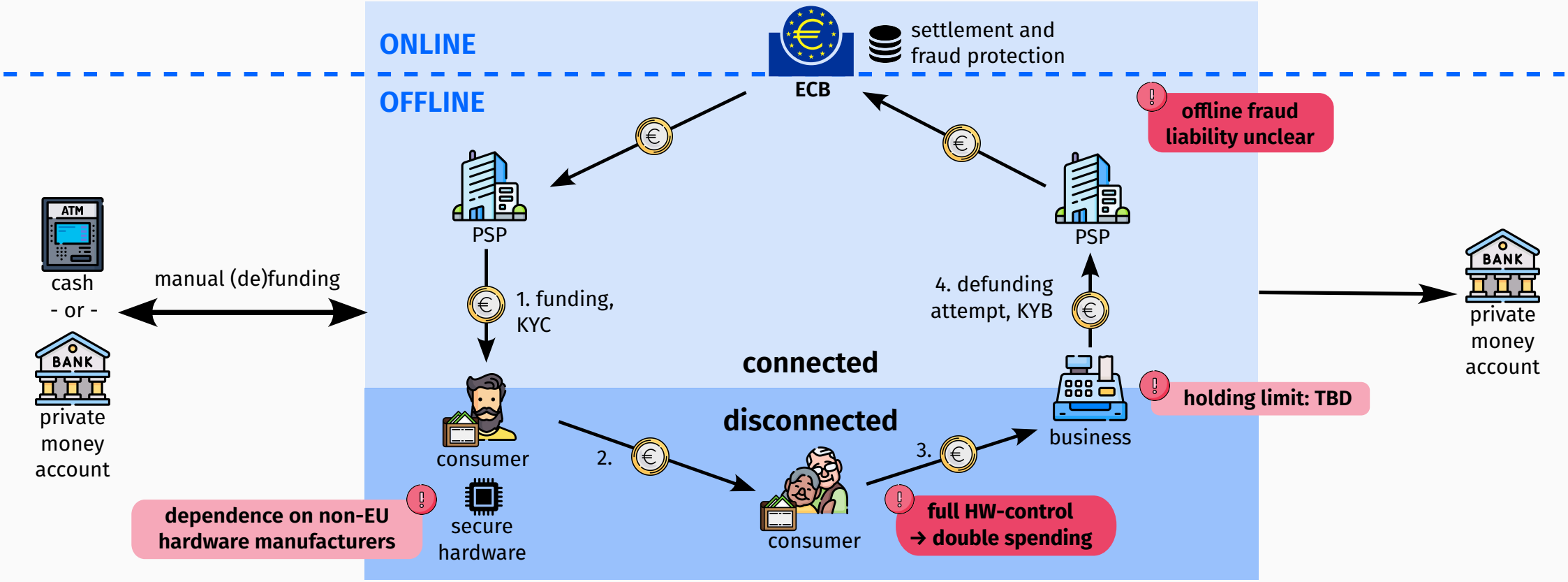
Offline Problems - Liability



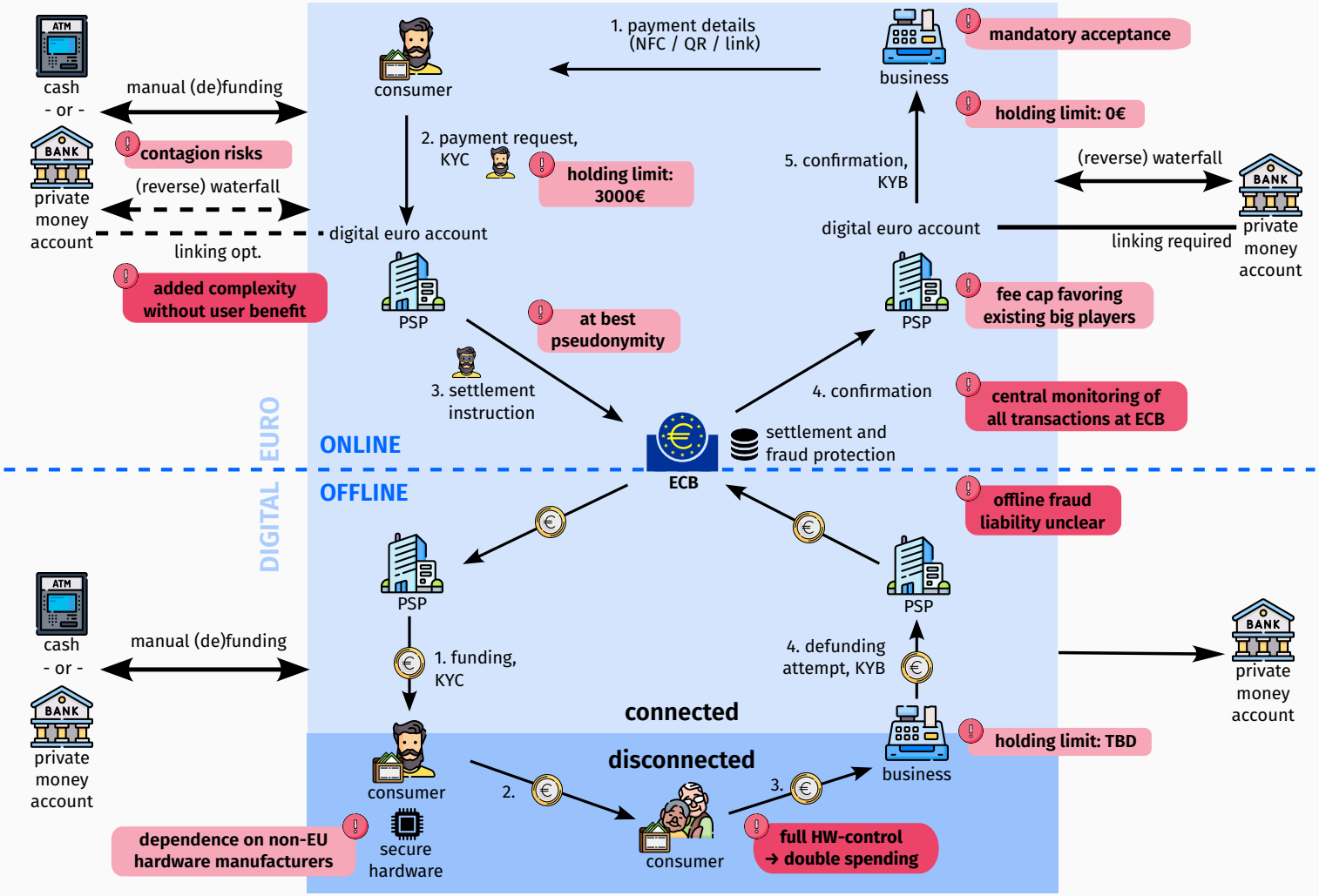
Offline Problems - Holding limit not determined



Offline Problems



Design Problems



Summary

Key Findings

1. Central monitoring of all online euro transactions by the ECB
2. Offline version is in strong conflict with HW-security, established CS results and full anonymity
3. Legal and financial liabilities remain unclear
4. Incentives for operators unbalanced; economical impact on merchants not adressed
5. No tangible benefits for society; online version duplicates existing systems
6. Exlusionary design process; critical design decisions done before public consultation.

References

[1] ECB, “FAQs on the digital euro.” [Online]. Available: https://www.ecb.europa.eu/euro/digital_euro/faqs/html/ecb.faq_digital_euro.en.htm

[2] ECB, “All news & publications (filtered search).” [Online]. Available: https://www.ecb.europa.eu/press/pubbydate/html/index.en.html?Taxonomy=Digital%20euro

[3] J. Cannataci, B. Fehrensen, M. Gütschow, Ö. Kesim, and B. Lucke, “Digital Euro: Frequently Asked Questions Revisited,” Jan. 26, 2026. [Online]. Available: https://arxiv.org/pdf/2601.18644

[4] S. Gilbert and N. Lynch, “Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services,” 2002, *ACM*. [Online]. Available: https://dl.acm.org/doi/epdf/10.1145/564585.564601

Acknowledgements

With funding from the:

Federal Ministry
of Research, Technology
and Space

https://concretecontracts.codeblau.de/

https://ngi.taler.net/

Questions?

1. Central monitoring of all online euro transactions by the ECB
2. Offline version is in strong conflict with HW-security, established CS results and full anonymity
3. Legal and financial liabilities remain unclear
4. Incentives for operators unbalanced; economical impact on merchants not adressed
5. No tangible benefits for society; online version duplicates existing systems
6. Exlusionary design process; critical design decisions done before public consultation.

Paper [3] available at