Report

Comparative analysis of technologies for CBDCs – a TNO perspective on the Digital Euro

An overview of potential technologies and standards for the Transaction Process Flow

Authors

David Otto
Abhishek Mahadevan Raju

TNO 2024 R11044

TNO innovation for life

Contents

Management Summary

This report navigates the reader to the evolving landscape of Central Bank Digital Currencies (CBDCs) in the European Economic Area (EEA), specifically focusing on the Digital Euro project. The primary objective is to clarify the fundamental concepts underpinning the digital euro, elaborate on potential technologies and standards, and explain the potential impact of architectural choices on the society. We are shedding light on what a CBDC is, discussing current developments, and outlining future plans, laying the foundation for a deeper understanding of their implications.

We narrowed our scope to the most significant process flow for the Digital Euro - the Transaction Process Flow, deconstructed into its fundamental building blocks. Drawing from our current knowledge, gleaned from the latest publications and pilot projects from the Digital Euro project, as well as similar explorations by various Central Banks, we provide an introduction to the spectrum of possible architectural choices for the building blocks of the Transaction Process Flow of a Digital Euro.

We explore critical building blocks such as Digital Identity, Transaction Initiation, Transaction Processing, and Settlement, dissecting each element's description, underlying technology and standards, as well as their anticipated impact on society in various dimensions, such as financial security, user trust (including privacy) and inclusion and openness. To facilitate this, TNO's expertise in areas such as Self-Sovereign Identity (SSI), Privacy-Enhancing Technologies (PETs), and Strategy & Policy (TNO Vector) enables a thorough understanding of the complexities involved in the Digital Euro's development.

Key takeaways:

1. It is expected that the Self-Sovereign Identity (SSI) ecosystem is of vital importance for **the digital identity**. Based on recent regulation related to a European Digital Identity, such identities are increasingly being designed for various use-cases. SSI ecosystem concepts are compatible with both centralized and decentralized implementations of a CBDC.
2. Privacy-Enhancing Technologies (PETs) encompass a range of digital technologies designed to protect sensitive information and safeguard the identities during the **transaction initiation** and **transaction processing** of the digital euro from malicious access.
3. **Settlement**, while a critical component ensuring finality and user trust in financial transactions, is generally not a technically intensive step in the process and technology choice has a minimal impact on end-users, whether in centralized or decentralized systems.
4. The **end-user adoption** depends on the impacts of the underlying technologies and standards that the Digital Euro will have, and should be considered for a successful roll out safeguarding citizens interest and concerns.
5. The choice between centralized and decentralized systems in digital currency ecosystems, which is the network of stakeholders and technologies enabling the creation, distribution, and use of a digital currency, is influenced by various factors, with user trust playing a significant role. Centralized systems may provide trust through standardized processes but raise **privacy concerns**.

   While decentralized systems empower users with greater control and transparency, it can face challenges in building user trust due to their novelty and could also have an impact on financial inclusion.
6. A **private blockchain** maintained by the ECB offers a promising path for achieving the Eurosystem's Digital Euro objectives in a decentralized manner with a strong focus on privacy and security, while supporting robust auditing and regulatory compliance.
7. The report provides a comprehensive overview of potential technologies and standards for the Digital Euro Transaction Process Flow. It underscores the importance of adopting a balanced approach and highlights that the **choice of technologies and standards**, whether centralized or decentralized, should be made **individually for each building block**, considering their respective advantages and impacts.

Figure 1 *The Transaction Process Flow of a CBDC and its technologies, standards and impacts*

	Digital Identity		Transaction Initiation		Transaction Processing		Settlement	
	Technologies & standards		**Technologies & standards**		**Technologies & standards**		**Technologies & standards**	
	• European Digital Identity (eIDAS 1.0 and 2.0) • European Digital Identity Wallet (EUDI) • Self-sovereign Identity (SSI) • Decentralized Identifiers (DIDs) • Qualified Electronic Signatures (QES)		• Know-Your-Customer (KYC), International Banking Account Number (IBAN) • Society for Worldwide Interbank Financial Telecommunication/Bank Identifier Code (SWIFT/BIC) • Global Legal Entity Identifier Foundation (GLEIF) • Account Information Services (AIS), Second Payment Services Directive (PSD2) • Verifiable Credentials (VCs) and DIDs • Verifiable Legal Entity Identifiers (vLEIs) • 5th Anti-Money Laundering Directive (5AMLD) • Markets in Crypto-Assets (MiCA)		• PSD2 & Payment Initiation Services (PIS) • ISO 20022 Standard for Financial Messages • IEEE 2143.1 - 2020 Procedure for Cryptocurrency Payments • ETSI GS PDL 011 pecifications for implementation of permissioned Distributed Ledgers - by ETSI Industry Specification Group for PDL (ISG PDL)		"The technology and standards depend on the role of the intermediaries in the transaction flow and may differ significantly based on decentralized and centralized approaches"	
Impact	**Centralized**	**Decentralized**	**Centralized**	**Decentralized**	**Centralized**	**Decentralized**	**Centralized**	**Decentralized**
Inclusion & Openness	🟢	🟢	🔴	🟢	🟠	🟠	"There is no direct impact on the end-user regarding the usage of technologies and standards, however it has to be reliable to ensure finality of a transaction and enhance user trust."	
Financial security	🟠	🟢	🔴	🟠	🟠	🟢		
User trust	🟠	🟢	🟠	🟠	🟢	🟠		

1 Introduction

The Digital Euro project, initiated by the Eurosystem under the guidance of the European Central Bank (ECB), is an ongoing endeavor to explore the implementation of a CBDC within the European Economic Area (EEA) as a response to the disruptive digital changes occurring in payment systems worldwide. The project is driven by a robust process involving prototyping exercises, market research, open contributions, and feedback solicitation. Through multiple pilot programs, the project evaluates the feasibility of various technologies, aiming to create a public digital payment system. The successful implementation of the Digital Euro is expected to foster financial inclusion, openness, financial security, and user trust (including privacy). However, the specific technologies to be employed in its design remain uncertain. By focusing on the key building blocks for the Transaction Process Flow - the everyday payment flow for the end users - we can gain valuable insights into the potential technologies, standards and their societal impacts.

It seems essential to involve knowledge centers capable of bridging the gap between societal impact and underlying technologies, ensuring a comprehensive understanding of the Digital Euro's implications. This next phase – the preparatory phase – began on November 1, 2023, and is planned to last 2 years with objectives of finalizing the digital euro rulebook, selecting development providers, and conducting testing to align with the Eurosystem requirements and user needs. TNO's expertise in areas such as Self-Sovereign Identity (SSI), Privacy-Enhancing Technologies (PETs), and Strategy & Policy (TNO Vector) enables a thorough understanding of the complexities involved in the Digital Euro's development. This report outlines potential technologies and standards - necessary for gaining an initial idea of the development context - and its impacts, crucial for understanding future societal implications. It navigates the reader through the complexity of the Digital Euro landscape.

2 Background

2.1 What is a CBDC?

A Central Bank Digital Currency (CBDC) is the umbrella term for all digital forms of a country's official currencies issued and regulated by a central bank, establishing a direct link with the national monetary authority. The specific design of this digital form of currency will mostly depend on policy objectives, whether it aims to ensure complete freedom for the user, retain full control of the financial system, or find a middle ground between the two. Despite varying design objectives, a CBDC always serves as a digital representation of physical cash, since it enables electronic transactions and peer-to-peer transfers. It differs from current electronic transactions by commercial banks since the actual value is stored in the electronic wallet of the user and is directly backed by the central bank. The direct backing by the central bank makes it legal tender. The legal tender status means that the currency must be accepted as a form of payment by law. This is also a crucial distinction from cryptocurrencies as this status ensures stability and confidence that comes with established monetary systems. Notable examples of CBDC initiatives can be found since 2020 in countries like Japan and Russia, where both nations have undertaken efforts to explore their own respective digital currencies, known as the Digital Yen and Digital Ruble.[1, 2]

2.2 Current developments

The European Central Bank (ECB) published their first comprehensive report also in 2020 that outlined the benefits, risks, and considerations associated with a Digital Euro. Building on this foundation, the Digital Euro project was officially announced by the Eurosystem in July 2021 to explore the Digital Euro for the European Economic Area. This investigation phase of the project ran from October 2021 to October 2023.[3] The project is a strategic initiative aimed at exploring the implementing of a Digital Euro under the supervision of the European Central Bank (ECB). The Digital Euro project has multiple objectives (see Table 1: Objectives of the Digital Euro), with its overarching goal: *Respond to the disruptive digital changes occurring in payment systems worldwide*. By leveraging CBDC technology, the project strives to achieve financial inclusion, openness, financial security, and user trust (which also includes privacy).[4] The European Commission also presented a legislative proposal dedicated to the

Table 1 *Objectives of the Digital Euro*

Objectives	
Preserving the role of public money as monetary anchor	**Respond to disruptive digital change of the payment systems worldwide**
Support the digitalization of the European Economy	
Strengthen the strategic independence of the European Union;	
Response to a significant decline in the role of cash as a means of payment,	
Avoid risks of unregulated payment solutions	
Pre-empting uptake of digital foreign currencies,	
And more...	

1 Central Bank Digital Currency : 日本銀行 Bank of Japan (boj.or.jp)
2 Consultation_Paper_201013_eng.pdf (cbr.ru)
3 Project and governance (europa.eu)
4 A further description of the impacts can be found in chapter 6

introduction of a Central Bank Digital Currency (CBDC) known as the Digital Euro. The proposal suggests that the Digital Euro will not be mandatory and will not have programmable features as a means of payment. The implementation of the Digital Euro as legal payment is yet to be voted on by the European Parliament and EU member states. If the law is passed, the European Central Bank (ECB) will have the authority to decide if and when the CBDC will be introduced. The involvement of various stakeholders, including financial institutions, governmental institutions, special interest groups, and the end users, is crucial in shaping the project's direction and ensuring that the Digital Euro will add value to all stakeholders including the society itself. The implementation of the Digital Euro can in this manner become a major breakthrough as it can disrupt many aspects of the society and current businesses practices. It can also have unintended impact as businesses may face challenges in integrating Digital Euro payment systems and the underlying technological infrastructure into their existing processes. Additionally, this adoption could involve significant upfront costs. Society, in this regard, would become increasingly reliant on digital devices, such as smartphones or computers, for financial transactions. Unfortunately, not everyone would have access to the necessary technology, which could lead to exclusion and further widen the digital divide.

As of 18th October 2023, the investigation phase of the Digital Euro project was concluded, signaling a green light to move forward with the preparatory phase. Throughout the investigation, the European Central Bank actively engaged with stakeholders including market participants, EU institutions, retail payment forums and policymakers, to identify the advantages and benefits of achieving a functional Digital Euro, and categorized multiple key priorities to ensure that the Digital Euro would prove to be beneficial and accessible, and assess the impact on the financial ecosystem. Prototyping exercises and stakeholder engagement through institutional discussion forums showed that a large pool of European providers possess the technical capability to support the Digital Euro infrastructure, and that numerous architectural choices are possible.

To further advance the project, the Digital Euro initiative also focuses on creating a comprehensive rulebook and developing initial reference architectural designs.[5] The Rulebook Development Group (RDG), representing different market participants, has been working on a draft rulebook for a Digital Euro scheme. The focus has been on creating use cases and user journeys that are appealing to end users and businesses. The RDG members will conduct an interim review of the first parts of the drafted rulebook in the first quarter of 2024, allowing stakeholders to provide feedback for potential adjustments. Subsequently, the draft rulebook will be finalized with additional chapters during the digital euro preparation phase.[6]

This next phase – the preparatory phase – began 1st November 2023, and is planned to last 2 years with the objectives of finalizing the Digital Euro rulebook, selecting development providers, and conducting testing to align with the Eurosystem requirements and user needs. Continuous engagement with the public and stakeholders will be prioritized during this phase, with the Governing Council reassessing the situation after two years to decide on the potential issuance and rollout of the Digital Euro. Important to note that no final decision has been made regarding which technologies and standards will be used for the Digital Euro – and such a decision will be made after the completion of the legislative process. The Governing Council of the ECB will decide on issuing a digital euro only after the adoption of the legislative act, with close monitoring of legislative debates and implementation of any necessary adjustments to ensure compliance with the legal framework.[7]

5 Mandate of the Digital Euro scheme Rulebook Development Group (europa.eu)

6 Update on the work of the digital euro scheme's Rulebook Development Group (europa.eu)

7 A stocktake on the digital euro - Summary report on the investigation phase and outlook on the next phase (europa.eu)

Stakeholders, including the readers of this report, are encouraged to actively keep track of the progress.[8] As mentioned earlier, the Digital Euro has the potential to disrupt various aspects of society and current business practices. However, it remains uncertain which specific technologies and standards will serve as the foundation for this digital currency, and consequently, the broader impact it might have. Some technologies, especially in the realm of cryptocurrencies, are also quite hard – if not impossible – to ignore, regulate or limit. It is paramount to find the best compromises and technologies to support European values while being in line with current regulations and allowing innovation at the same time. Pilot programs with active consumer use of the Digital Euro are expected to commence around 2025. This year is a highly opportune time to provide feedback towards the Digital Euro project, and to propose the inclusion of secure technologies and standards in the architecture of the Digital Euro. Therefore, this report focuses on a comparative analysis of various technologies, standards and its impacts for the Digital Euro (see chapter 5).

8 Project and governance (europa.eu)

3 The scope of the comparative analysis

3.1 Overview

CBDC's wide societal impact is discussed by focusing on the design of Retail CBDCs, intended for usage by end-users. Furthermore, the comparative analysis is focusing on CBDC as an account-based token. An account-based token, closely resembling the current financial ecosystem, represents ownership or access rights tied to a specific account or identity, just like traditional banking and financial systems.

A comparative analysis of technologies and standards towards the Digital Euro requires:

- Look at specific components/building blocks that fulfill a primal function; the Transaction Process Flow.
- In-depth understanding of the current design choices under consideration for the Digital Euro and from other CBDC initiatives; centralized- and decentralized approaches.
- Defining the impacts derived from the objectives of the Digital Euro.
- Describing each building block of the Transaction Process Flow in more detail
- Analyze technologies and standards categorized on their centralized- and decentralized approaches for each building block.
- Understanding the societal impact of these technologies for each building block on centralized and decentralized approaches.
- Define the key takeaways from the above mentioned analyses.

These will be addressed in the following sections.

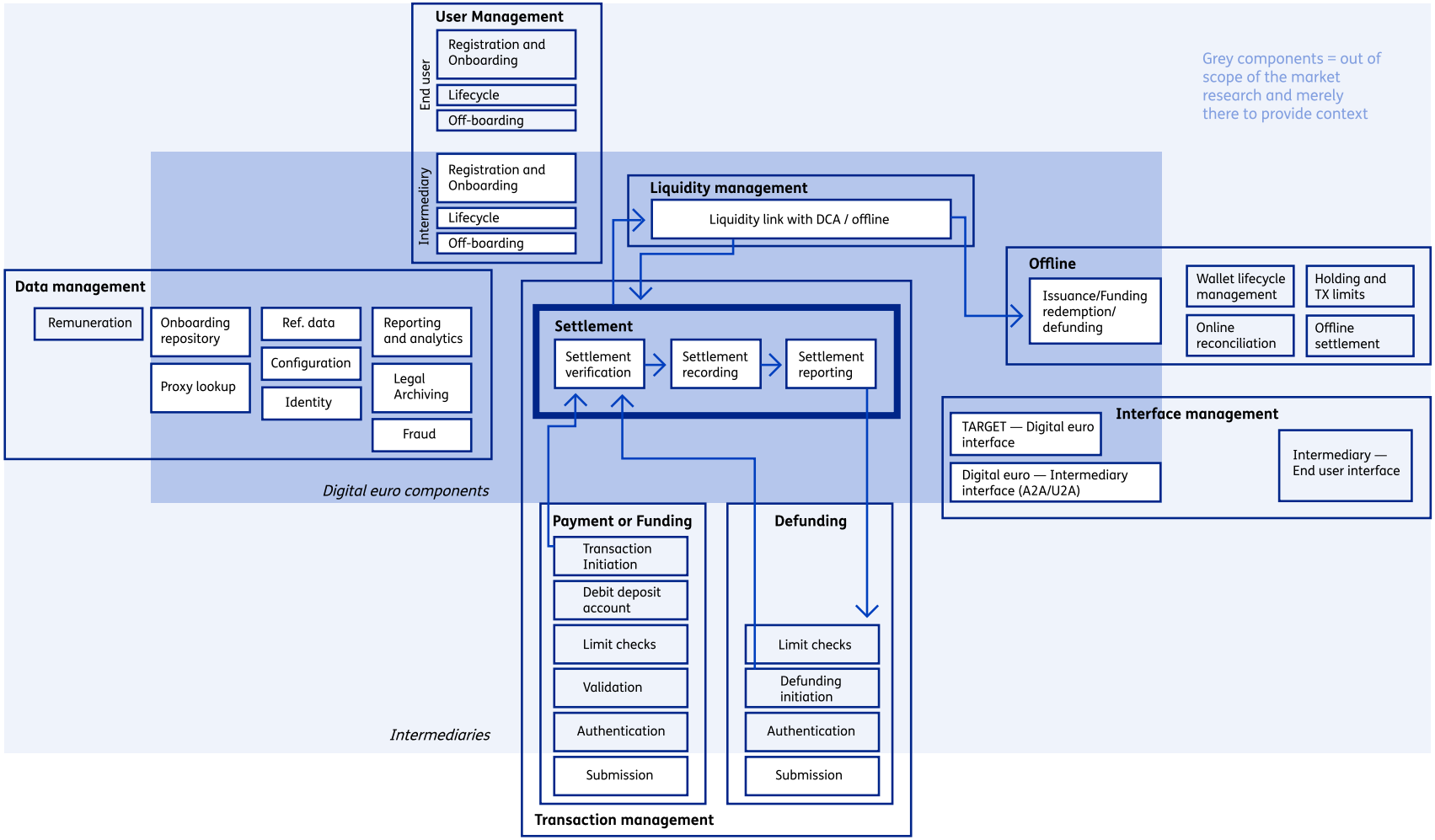
3.2 The Transaction Process Flow

As a part of the investigation phase within the Digital Euro project, the Eurosystem conducted a market research to solicit industry feedback on various design proposals for the Digital Euro. The objective was to gather valuable insights from stakeholders and market participants about the development and necessary components of the digital currency.

On 26th May 2023, the Eurosystem published the outcome of this research exercise, presenting a comprehensive report that aggregated insights related to 12 diverse supporting components. The report detailed end-to-end flows between various actors, encompassing crucial aspects like onboarding procedures and transaction flows. During this exercise, the Market Advisory Group created potential versions of the Digital Euro's design, which served as a valuable input into the overall research findings. The design proposal included various components, aspects and considerations of the Digital Euro, which can been seen in the figure on the next page.

Figure 2 on the next page illustrates the intricate interplay between various components, each comprising a multitude of functionalities and sub-functionalities within the Digital Euro system. It is important to acknowledge that this figure presents a preliminary version, and ongoing investigations by the Digital Euro task force aim to refine this map into a more definitive and comprehensive version. The Rulebook Development Group will play a crucial role in this process, delineating the roles and responsibilities of different actors involved in managing each functionality.

Figure 2 *Functional and non-functional component map in the Digital Euro ecosystem*[9]



9 Source: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf

This report will delve into the Transaction Process Flow, recognizing it as the core end-to-end functionality for end-users.

The selection of the transaction flow design for our analysis is driven by three compelling reasons.

- The widespread adoption of a Digital Euro hinges on the presence of a well-crafted payment system capable of catering to the daily needs of millions of end-users. Such a system must ensure a seamless, secure, and efficient transaction process while accommodating a diverse range of functionalities, for example portability and offline capabilities to enhance inclusivity, particularly in hard-to-reach areas.
- As highlighted in Chapter 2, challenges surrounding the Digital Euro payment systems arise not only in the context of business practices but also in the broader societal reliance on these systems. An optimal transaction flow system must be devised to promote interoperability and careful rollouts.
- The infrastructural design of the Transaction Process Flow will exert far-reaching effects on other building blocks within the Digital Euro component map (see The Transaction Process Flow Figure 2). For instance, supporting offline transactions may pose complexities in a system where registering transactions relies on cloud-based components. Making informed decisions about the Transaction Process Flow infrastructure is important as it lays the groundwork for an interconnected and efficient Digital Euro ecosystem, shaping the success and usability of the Digital Euro.

The Transaction Process Flow can be viewed from various perspectives and adapted to different use-cases. In Figure 3 and 4, we outline two such use-cases, referenced from the Digital Euro Market Advisory report, providing insights into how the Transaction Process Flow operates in different scenarios.

In both use-cases above, end-users initiate the transaction, and intermediaries and Digital Euro infrastructure components help validate and settle the transactions. Based on this information, building blocks could be determined for the entire Transaction Process Flow. The building blocks of this process flow are illustrated in Figure 5.

Figure 3 *Payer-initiated flow*[10]

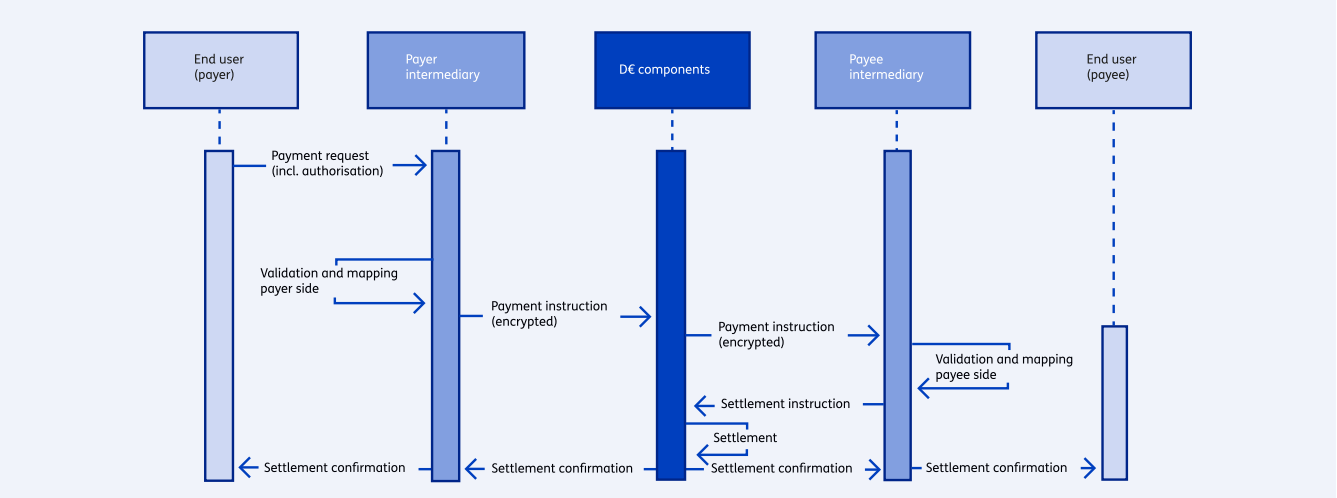
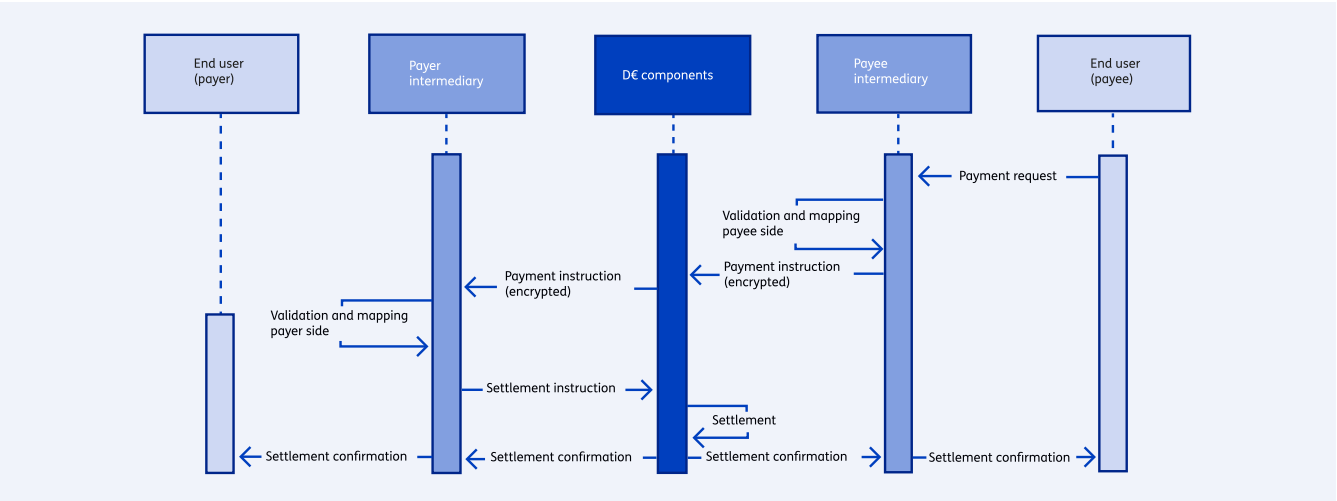


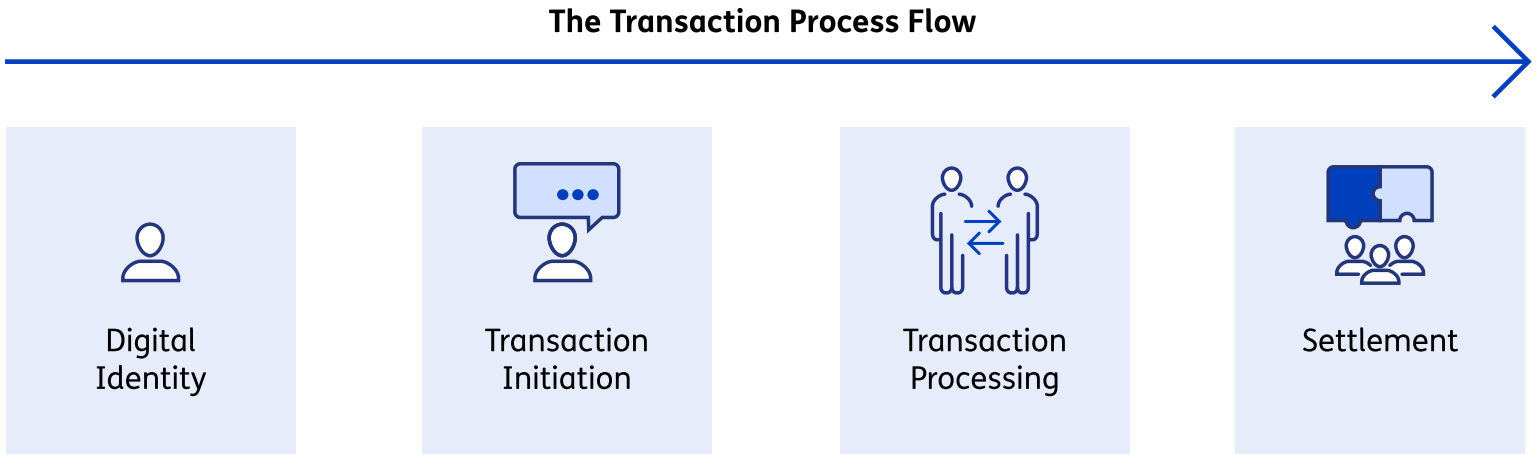
Figure 4 *Payee-initiated flow*[11]



10 Source: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf

11 Source: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs230113_Annex_1_Digital_euro_market_research.en.pdf

Figure 5 *Building blocks for the Transaction Process flow*

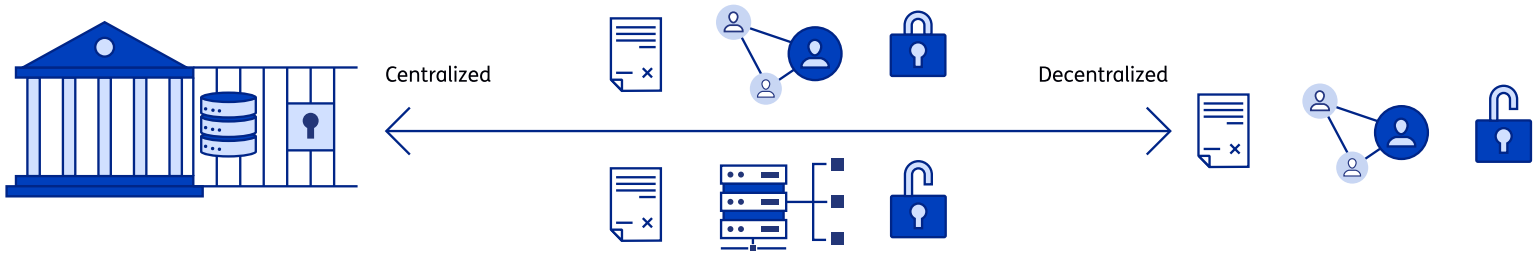


3.3 Technology Overview

For each of these building blocks (see Figure 5), we conduct an analysis of the associated technologies and standards. When considering the technologies and standards for Central Bank Digital Currency (CBDC) initiatives, it's important to recognize that these initiatives generally follow two primary approaches: centralized and decentralized. In a centralized CBDC approach, a central bank maintains complete control over the issuance, distribution, and validation of transactions, much like traditional fiat currencies. The system typically relies on a permissioned blockchain or a centralized database managed by the central bank or a consortium of trusted financial entities. In contrast, a decentralized CBDC operates on a permissionless blockchain, allowing for a distributed network of nodes to validate transactions. This design closely resembles the structure and behavior of traditional cryptocurrencies.

The spectrum of choices for defining the Digital Euro is illustrated in Figure 6, presenting various degrees of centralization and decentralization in its infrastructure and control for the Digital Euro. On the left side of the axis, a fully centralized approach is similar to a traditional Web 2 model, with a large centralized data center owned and operated by the European Central Bank (ECB). This design emphasizes centralized control over the entire Digital Euro system. Conversely, on the right side of the axis, a fully decentralized approach involves the Digital Euro functioning as a smart contract on a public blockchain. In this scenario, there are no privileged functions, ensuring that no individual or entity possesses special access to functionalities within the smart contract, mimicking the principles of cryptocurrencies like Bitcoin and Ethereum.

Figure 6 *Spectrum of choices for CBDC Infrastructure*



While these two examples represent the extreme ends of the spectrum, there exist various hybrid options depending on the technologies chosen for each of the building blocks in the Digital Euro system. The design choices will significantly influence the degree of centralization or decentralization, privacy features, scalability, and security of the Digital Euro

Centralized CBDC attempts have seen considerable progress, with numerous countries piloting or implementing their own systems. For instance, China has been at the forefront of developing a digital yuan, commonly known as the Digital Currency Electronic Payment (DCEP) system[12]. China's DCEP operates on a two-tiered system, where the central bank issues the digital currency to commercial banks, and these banks further distribute it to the public. The central bank retains full control over the issuance and validation of transactions, enhancing monetary policy implementation and combating illicit activities. Similarly, in Sweden, the

12 In Search of The Perfect Coin: China's Approach towards Cryptocurrency and Its Own Central Bank Digital Currency (August 2021), Xia, Mian

Riksbank is actively exploring the e-krona[13], a partially-centralized CBDC built on the Corda blockchain platform, ensuring faster and more secure transactions within a controlled ecosystem. While centralized CBDCs offer robust regulatory oversight, they raise concerns regarding data privacy, as central authorities could maintain access to sensitive transactional data.

Conversely, the concept of decentralized CBDCs is relatively novel and still in experimental stages. This approach allows for financial inclusion in remote areas where traditional banking infrastructure is lacking. Beyond inclusion, such a system can also be found to be significantly scalable and reliable. The Bank of Japan has successfully completed multiple proof-of-concept tests on basic ledger-based functions on a CBDC system[14]. A Digital Yen blueprint is currently in development, in collaboration with private-sector collaborators[15]. Similarly, the Bank of Russia is also launching pilot programs with the Digital Ruble, and plans for the system to be widely available to the public by 2025. Additionally, the decentralized nature ensures enhanced resilience and transparency, reducing the risk of single points of failure. However, decentralized CBDCs face hurdles related to high-scalability and transaction speed, as the consensus mechanism must handle a higher number of transactions compared to centralized models.

The choice of the underlying technologies and standards plays a pivotal role in shaping the Digital Euro's impact on society. A fundamental aspect of the Digital Euro's architecture lies in the spectrum of design approaches, particularly concerning the degree of centralization or decentralization. This spectrum encompasses considerations related to control and infrastructure, reflecting divergent perspectives on the optimal level of centralization or decentralization for the Digital Euro. Striking the right balance in this regard is crucial to avoid any unforeseen consequences and ensure the Digital Euro's successful integration into the financial ecosystem while addressing societal needs effectively.

13 https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2023/work-on-e-krona-entering-new-phase

14 Bank of Japan: Central Bank Digital Currency Experiments - Results and Findings from "Proof of Concept Phase 2"

15 https://www.reuters.com/technology/boj-launches-forum-with-60-firms-digital-yen-pilot-programme-2023-07-20

3.4 Impacts

The assessment of the impacts derived from the objectives mentioned in the reports of the Digital Euro project[16] is crucial in guiding the selection of appropriate technologies for each building block. The following key impacts are considered, with a focus on inclusion and openness, financial security, and user trust (including privacy):

Inclusion and openness

The choice of technology should promote financial inclusion, ensuring that all citizens have access to the Digital Euro, regardless of their digital literacy, socioeconomic status or geographical location. Openness in the design allows for interoperability with existing financial systems and technologies, fostering seamless integration and widespread adoption. Offline solutions facilitate access to the financial ecosystem in locations with poor network access.

Financial security

The chosen solutions must be robust and resilient, safeguarding the Digital Euro against cyber threats, fraud, and counterfeiting. The use of secure and tamper-proof cryptographic protocols, multi-factor authentication, and data encryption are essential considerations to ensure the integrity and trustworthiness of the digital currency. A key priority for the Digital Euro project is to minimize the impact to the existing financial infrastructure as well, and the ripple effects of the network must be considered and tested in pilot projects.

User trust (including privacy)

Building user trust is vital for the successful adoption of the Digital Euro. Technologies should prioritize privacy, protecting users' sensitive financial information while complying with regulatory requirements – such as anti-money laundering (AML) and know-your-customer (KYC) standards. Transparent and auditable processes can enhance user confidence in the system.

Strategy & Policy

A key objective of the Digital Euro task force is to minimize negative impact of the Digital Euro's rollout on not only the existing financial infrastructure but also the society, allowing optimal inclusion, openness, financial security and user trust (including privacy). This could potentially lead to scalability of the Digital euro project and a significant increase of users safeguarding all their interests and concerns. This requires meticulous analysis of possible innovation strategies and impact analyses of technologies and standards to ensure that such rollouts may be successful, e.g. Systeemanalyse[17], AI-usage by the public sector[18].

17 https://vector.tno.nl/expertises/systeemanalyse/

18 Quick scan AI in de publieke dienstverlening | Rapport | Rijksoverheid.nl

Technologies and standards will be evaluated on these impacts based on their centralized and decentralized approaches. In this report we particularly focus on the impacts within a certain building block for centralized and decentralized approaches. This evaluation is conducted for each of the building blocks of the Transaction Flow.

16 Report on a digital euro (europa.eu)

4 The comparative analysis for the Transaction Process Flow

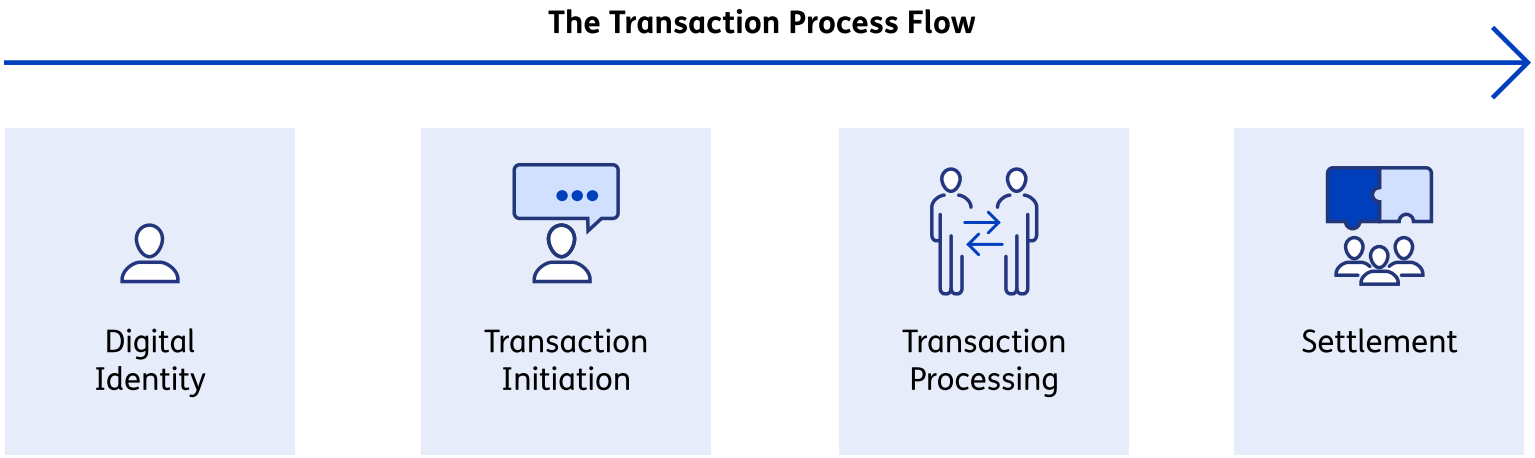
4.1 Overview

In the previous chapter, we set the groundwork by contextualizing and scoping our research regarding the Digital Euro framework. In this chapter, we will focus on each of the building blocks of the Transaction Process Flow, a crucial element at the core of CBDCs and also for the Digital Euro's functionality. This chapter delves into the fundamental building blocks that constitute the transaction process, its underlying technologies and standards that shape infrastructural choices. Additionally, we explore the implications of opting for either the centralized or decentralized side of the spectrum, and shedding light on how this choice can profoundly impact the inclusion, financial security, and user trust(including privacy) of the Digital Euro system.

4.2 The Building Blocks

The Building Blocks of the a Transaction Process flow are identified in the previous chapter and shown again below in Figure 7. These building blocks are further explained in subsequent sections.

Figure 7 *Building blocks for the Transaction Process flow*



4.3 Digital Identity

4.3.1 Description

Digital identity is a foundational building block of the Digital Euro, serving as a standardized representation of individuals, applications, or machines within the digital realm. Focusing primarily on individuals, the digital identity framework encompasses a diverse spectrum of attributes, including personal information, credentials, relationships, and permissions. As the digital identity framework evolves, the integration of these initiatives will play a crucial role in shaping the Digital Euro's efficacy and user experience, establishing a robust and unified identity infrastructure for the digital economy.

In the European context, the European Digital Identity[19] (EUDI) Wallet and their European Digital Identity[20] initiatives are of significant importance. The EUDI Wallet aims to provide a user-centric and privacypreserving solution, enabling individuals to control and manage their European digital identity securely. Although transactions of a digital euro

19 EUDI – European Digital Identity - Press Release, Pilot Projects, EUDI Wallet Architecture and Reference Framework (ARF)

20 European Digital Identity Initiative

could occur offline, like cash, eliminating the need for an intermediary and avoiding the processing of personal or transactional data, privacy advocacy groups still express significant concerns about digital identities lack of anonymity. On the other hand, the European Digital Identity initiative to empower citizens with a single, trusted, and interoperable digital identity that can be utilized across various online services and transactions. This wallet will not only enhance user convenience but also strengthen the overall security of digital interactions within the Digital Euro ecosystem. Additionally, the implementation of the Digital Euro Digital Identity could addresses concerns regarding the maximum amount for identification and the ability to track the number of accounts associated with an individual. Moreover, the broader European Digital Identity initiative seeks to foster the acceptance and recognition of digital identities across the European Union, promoting seamless and secure cross-border transactions while reinforcing trust in digital services.

4.3.2 Supporting Technology and Standards

4.3.2.1 Centralized

The electronic Identification, Authentication and Trust Services (eIDAS) 1.0 Regulation[21], which governs electronic identification and trust services within the European Economic Area (EEA), currently plays a significant role in the context of the centralized digital identity approach for the European Digital Identity Wallet. The eIDAS regulation ensures the cross-border recognition and acceptance of national electronic identification (eID) schemes among EEA member states, enabling citizens to use their eIDs from one country to access public services online in other EEA countries. This facilitates a seamless and secure authentication process for individuals, enhancing user convenience and promoting interoperability across the Digital Euro ecosystem.

Under the centralized model, the European Digital Identity Wallet would adhere to eIDAS-compliant national eID schemes, such as DigiD[22] in the Netherlands. Once a national eID scheme is recognized at the European level, it becomes usable in other EEA countries. This enables individuals to access Digital Euro services and conduct transactions with their eID from their country of origin, promoting a unified and standardized approach to digital identity within the EEA. By leveraging eIDAS and adhering to its framework, the centralized digital identity approach ensures a secure and reliable source of identity data, enhancing user trust and acceptance while facilitating cross-border digital interactions within the European Union.

In the context of the Digital Currency, centralized approaches such as the eIDAS 1.0 provide stability and interoperability throughout the European Union, and are actively being used.

4.3.2.2 Decentralized

Self-Sovereign Identity (SSI)[23] is a significant development in autonomous digital identity solutions, with interesting solutions for the digital identities. SSI empowers individuals with control over their identity information, aligning harmoniously with the principles mandated by eIDAS 2.0[24], a revision of the original regulations. Utilizing a decentralized approach, SSI places the end-user at the center of their digital identity, giving them exclusive ownership and agency over their identified attributes within the digital currency ecosystem, which is the network of stakeholders and technologies enabling the creation, distribution, and use of a digital currency.

21 Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions
22 DigiD
23 Self-Sovereign Identity in the context of eIDAS
24 eIDAS 2.0

In the context of the digital currency realm, Decentralized Identities (DIDs)[25] are a core aspect of eIDAS 2.0. Rooted in the principles of SSI, DIDs demonstrate a user-centric and privacy-preserving paradigm, granting individuals full autonomy over their identity management in the digital currency ecosystem. In the eIDAS 2.0 framework, DIDs offer an inclusive framework wherein any participant, spanning individuals, businesses, and residents within the digital currency network, can access the advantages of a secure and interoperable digital identity infrastructure.

The decentralized design of DIDs places emphasis on conferring users authority and privacy over their digital identities, aligned with data protection regulations, including the General Data Protection Regulation (GDPR).[26] Through this empowerment, DIDs embody a flexible and adaptive identity system supporting migration and autonomy, something not available in conventional identity frameworks. The empowerment of end-users allows increased levels of trust, which in turn can spur the widespread adoption of digital currencies among European Union (EU) citizens.

Significantly, DIDs facilitate the issuance of Qualified Electronic Signatures (QES)[27] across the digital currency ecosystem, affording robust security features during storage and service application. The cryptographic proofs harnessed by DIDs empower users to authenticate selected, pertinent identity attributes required for specific transactions, thereby ensuring a high degree of authenticity while safeguarding customer privacy. Self-Sovereign Identity wallets are also a key part of the new regulation, thus supporting the usage of DIDs to sign credentials proving identity.

25 DID-Core W3C Specifications
26 GDPR Information Home
27 Qualified Electronic Signatures in the context of eIDAS

Self-Sovereign Identity

To support the implementation of CBDCs, it is expected that the Self-Sovereign Identity (SSI) ecosystem is of vital importance. Decentralized Identifiers (DIDs) in SSI are supporting digital identities for diverse use-cases. Based on recent regulation related to a European Digital Identity, such identities are increasingly being designed for various use-cases, such as the EUDI Wallet, and various governmental initiatives such as European Blockchain Services Infrastructure (EBSI).[28] SSI ecosystem concepts are compatible with both centralized and decentralized implementations of a CBDC. Examples of projects of TNO are eSSIF-Lab[29], EASSI initiative[30], SURF: Assisted in the design of an SSI-based IAM framework[31],[32], SSI Investigation for BZK done in collaboration with Innovator.[33]

28 What is EBSI?
29 eSSIF-Lab | eSSIF-Lab
30 TNO EASSI can accelerate SSI adoption | TNO
31 HOSA domeinarchitectuur Identiteit en Toegang (surf.nl)
32 technical-exploration-ssi-wallet-for-education-and-research.pdf (surf.nl)
33 pdf (overheid.nl)

4.3.3 Impact

4.3.3.1 Inclusion and Openness

Centralized systems:

- Offer a standardized and streamlined identity verification process, potentially increasing efficiency and reducing redundancies.
- Ensure regulatory compliance and oversight, mitigating the risk of fraudulent activities and enhancing consumer protection.
- Provide a single point of access for identity verification, simplifying user onboarding and minimizing user friction.
- Facilitate rapid deployment of digital currency services and updates, promoting quicker adoption and responsiveness to market demands.
- May lead to concerns about data privacy and misuse of sensitive information, potentially limiting user trust and participation.

Decentralized systems:

- Enhance inclusion by providing access to financial services for underserved populations, who may not have access to traditional identity verification methods.
- Empower individuals to control their identity data, promoting autonomy.
- Enable cross-border access to digital currency services without relying on centralized authorities, promoting financial inclusivity globally.
- Encourage collaboration and interoperability among diverse stakeholders, fostering an open and inclusive digital currency ecosystem.
- Increase interoperability efforts as identity systems may become complex and require more specific expertise to maintain.
- Digital illiteracy problem can result in improper management of private keys, leading to issues such as key loss, and not able to use their digital identities.

4.3.3.2 Financial Security

Centralized systems:

- Offer streamlined identity verification processes, potentially reducing instances of financial fraud and improving overall financial security.
- Facilitate seamless integration with existing financial infrastructures and regulatory frameworks, enhancing the overall security and efficiency of financial transactions.
- Can pose a potential target for cyber-attacks, making it crucial for robust security measures to be implemented to safeguard financial information and protect against potential vulnerabilities.
- May also raise concerns about data privacy and misuse, which could impact citizens' trust and confidence in the financial system, due to the reliance on centralized authorities.

Decentralized systems:

- Enhance financial security by reducing the risk of single points of failure and potential large-scale data breaches, which can have significant financial implications for countries and entities.
- Empower individuals with control over their identity data in a decentralized system and thus reduce the likelihood of identity theft and fraudulent activities, contributing to enhanced financial security for citizens.
- Are less susceptible to centralized cyber-attacks, safeguarding the stability and integrity of the existing financial system, due to the distributed nature of decentralized digital identities.
- Digital illiteracy can result in sharing information with unauthorized parties collectively jeopardize users' control over their digital identities and assets, and identity fraud.

4.3.3.3 User Trust (including privacy)

Centralized systems:

- May instill user trust through standardized and well-established identity verification procedures, providing a familiar and reliable experience for individuals.
- Can offer convenience and simplicity for users, as they can access multiple services through a single point of authentication, potentially promoting trust in the overall digital currency ecosystem.
- Could significantly erode public trust in the financial system and digital currency services, in the case of any breaches or mishandling of data. The potential risks associated with centralized data storage may raise concerns among users about the privacy and security of their identity information, impacting their willingness to fully embrace digital currencies and the underlying financial infrastructure.
- Concerns about improper surveillance by law enforcement of digital identities and further investigation into digital identities and their associated financial information.

Decentralized systems:

- Foster user trust by providing individuals with greater autonomy and sovereignty over their personal data, alleviating concerns about potential misuse or unauthorized access.
- Empower users with the ability to selectively share only essential identity attributes in a decentralized system, engendering a higher sense of security and confidence, encouraging wider adoption of digital currencies among citizens.
- Enhance user trust in the financial system, as transactions and identity verifications are recorded in a tamper-resistant manner, reducing the risk of fraud and enhancing the overall integrity of the digital currency ecosystem, because of the transparency and immutability offered by decentralized blockchain technology.

Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PETs) encompass a variety of digital technologies to protect sensitive information from malicious access. Such technologies may encompass techniques such as Data Obfuscation, as well as Trusted Execution Environments, and may be considered important to a potential CBDC architecture. Such architectures, either centralized or decentralized, may integrate approaches such as Selective Disclosure, Differential Privacy, Homomorphic Encryption and Multi-Party Computation. An exploration of various PETs is outside the scope of this report, but it is relevant to mention that some major DLT initiatives such as Ethereum already utilize Zero-Knowledge Proofs to protect the identities of transaction participants. E.g. Heracles[34], NICPET[35] or the Early Research Programme (ERP) in next generation crypto[36], and Multi Party Computation for Anti Money Laundering (MPC4AML)[37]

34 HERACLES project voor benutten gezondheidsdata van start (tno.nl)

35 Authorities learn with NICPET to leverage secure data sharing (tno.nl)

36 TNO's Early Research Programme in Next Generation Crypto · dcypher

37 TNO, Rabobank and ABN AMRO work on privacy-friendly data analysis | by ABN AMRO | ABN AMRO Developer Blog | Medium

4.4 Transaction Initiation

4.4.1 Description

Transaction initiation in the context of a CBDC involve two key aspects: entity resolution and onboarding. Entity resolution refers to the identification and verification of transacting parties in a digital currency ecosystem. It encompasses the resolution of unique digital identities for individuals, businesses, and other entities participating in CBDC transactions. Robust entity resolution mechanisms are essential to ensure the integrity and security of the digital currency network, mitigating the risk of fraudulent activities and enhancing user trust.

Onboarding is another pivotal component of transaction initiation, encompassing the process of registering and authorizing individuals and entities to access CBDCs services. It involves validating the identity and credentials of prospective users, ensuring compliance with regulatory requirements and know-your-customer (KYC) protocols. Efficient onboarding procedures are instrumental in facilitating seamless and inclusive participation for a digital currency ecosystem, supporting financial inclusion and fostering the widespread adoption of digital currency services. For the purposes of this analysis, we do not address the various forms of onboarding, as they may differ based on implementation and format.

4.4.2 Supporting Technology and Standards

4.4.2.1 Centralized

Various centralized identity resolution approaches play crucial roles in ensuring secure transactions within the digital currency ecosystem. These established systems, such as Know-Your-Customer (KYC), International Banking Account Number (IBAN), Society for Worldwide Interbank Financial Telecommunication/ Bank Identifier Code (SWIFT/BIC), and the Global Legal Entity Identifier Foundation (GLEIF)[38], leverage standardized protocols to verify the identities of transacting parties and facilitate seamless cross-border transactions while maintaining robust financial security. Additionally, the concept of Account Information Services (AIS) introduced by the Second Payment Services Directive (PSD2)[39] is a pivotal component within this framework.

KYC serves as a cornerstone for authenticating the identities of CBDC users, ensuring that participants are genuine and their identities properly documented. AIS empowers authorized third-party providers (TPPs) to access and aggregate customers' financial data across various accounts, providing a holistic view of transactions and balances. This consent-based approach enhances financial transparency, promoting customer-centric services while safeguarding data security and privacy.

IBAN, the standardized system for identifying bank accounts across borders, facilitates accurate cross-border payments, minimizing errors in international money transfers. The SWIFT/BIC system assigns unique codes to financial institutions, enabling swift identification during international transactions. Integrating these systems into the CBDC architecture streamlines onboarding and transaction processes, ensuring efficient and secure financial operations.

Additionally, GLEIF assigns unique identifiers known as Legal Entity Identifiers (LEIs) to entities participating in financial transactions. GLEIF enhances transparency and regulatory compliance by providing a standardized identification mechanism for entities engaged in financial activities.

4.4.2.2 Decentralized

As traditional centralized systems present challenges of data privacy, interoperability, and ownership, emerging technologies such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)[40] provide innovative solutions. DIDs, coupled with VCs, empower individuals to manage and

38 GLEIF
39 PSD2 Overview
40 Verifiable Credentials Data Model W3C Specifications

control their digital identities, enabling secure interactions while preserving data privacy. This approach fosters inclusivity, transparency, and user-centricity.

Additionally, the use of Self-Sovereign Identity (SSI) principles introduces a paradigm shift in identity management. With SSI, individuals retain ownership of their identity data and share it selectively, enhancing privacy and reducing the risk of identity fraud. Combined with DID-based authentication, SSI offers a decentralized alternative to traditional identification methods, creating a robust foundation for secure CBDC transactions.

Furthermore, novel concepts such as verifiable LEIs (vLEIs)[41], also from GLEIF introduce decentralized organizational identity verification – without reliance on a centralized verification authority. vLEIs leverage blockchain technology and Verifiable Credentials to establish a secure, tamper-resistant organizational identity that can be verified without intermediaries. This decentralized model enhances transparency in financial transactions, streamlining cross-border operations while maintaining data integrity.

In the scope of regulations, the 5th AML Directive (5AMLD)[42] extends anti-money laundering and KYC directives to cryptocurrency exchanges in the EEA, providing a framework of safety and regulatory compliance for cryptocurrency businesses. Similarly, the Markets in Crypto-Assets (MiCA)[43] is a regulatory proposal within the European Union's Digital Finance package.[44] It aims to create a comprehensive framework for regulating crypto-assets and related activities in the EU, with a focus on promoting innovation while ensuring consumer protection and mitigating risks. MiCA is part of a broader effort to embrace digital finance and blockchain technology, alongside proposals for a pilot regime on distributed ledger technology (DLT) market infrastructures and amendments to existing financial services rules.

4.4.3 Impact

4.4.3.1 Inclusion and Openness

Centralized systems

- Can streamline entity resolution by maintaining a centralized database of user information, potentially making it easier to implement uniform identity verification standards and ensure inclusivity.
- May hinder openness by concentrating control in the hands of a central authority, limiting competition and innovation in the entity resolution process.
- Could lead to exclusion if individuals or entities without access to the centralized system are unable to participate in CBDC transactions, potentially creating financial disparities.

Decentralized systems

- Promote openness by distributing entity resolution responsibilities across a network of participants, allowing for a more diverse set of entities to engage in the process.
- Enhance inclusion as they enable a broader range of identity verification methods, potentially accommodating users who may not fit into standardized centralized identity models.
- Might introduce complexities and interoperability challenges if various decentralized identity solutions are used, potentially excluding users who struggle with these complexities because of a low digital literacy.

41 Introducing vLEIs
42 EU Directive towards anti-money laundering and prevention of terrorist financing
43 EU Regulation on markets in crypto-assets
44 EU Digital Finance package

4.4.3.2 Financial Security

Centralized systems
- Can provide a sense of financial security to end-users due to established security protocols and the presence of a single trusted entity responsible for safeguarding data.
- Are vulnerable to systemic risks, as a single breach or attack on the central database could have widespread financial repercussions, eroding confidence in the CBDC ecosystem.
- May be prone to insider threats, where malicious actors within the central authority could misuse user data for financial gain, undermining trust.

Decentralized systems
- Enhance financial security by reducing single points of failure, making it more difficult for malicious actors to compromise the entire system.
- Could introduce security challenges related to the management of decentralized identity information, including the potential for data breaches in distributed networks.
- Require users to take more responsibility for their own security, which can be empowering but also pose risks if individuals are not well-informed or lack technical expertise.

4.4.3.3 User Trust (including privacy)

Centralized systems
- Inspire user trust through established protocols and oversight by a central authority, which can provide a sense of reliability and accountability.
- May erode user trust in the event of a data breach or misuse of personal information, leading to concerns about privacy and security.
- Can build trust through transparent identity verification processes, where users can see how their data is used and protected.

Decentralized systems
- Foster user trust by offering greater control over personal identity data, reducing the reliance on centralized authorities, and potentially enhancing privacy.
- May face challenges in building trust due to the novelty and complexity of decentralized identity systems, requiring education and awareness efforts.
- Empower users to have a more active role in their digital identity (either directly or through reliance on trusted service providers), which can lead to greater trust if implemented correctly, but also pose risks if individuals mishandle their own data.

4.5 Transaction Processing

4.5.1 Description

For the purposes of our definition and impact analysis, we separate the steps of a financial transaction resolution into two steps: the first step being the Transaction Processing, and the second being the Settlement (addressed in the following section). In the context of the Digital Euro, Transaction Processing is the core of the workflow, and may optionally be managed through subsidiaries.

In essence, Transaction Processing encompasses the transfer of funds from the payer's account to the payee's account. This also ensures that the payment is recorded accurately and instantaneously, reducing the risk of errors or delays commonly associated with traditional settlement methods. Instant settlement, a crucial aspect for users, plays a significant role in enhancing the efficiency and convenience of transactions. In an account-based CBDC, centralized CBDC architectures may be significantly similar to those supporting non-CBDC currencies.

4.5.2 Supporting Technology and Standards

4.5.2.1 Centralized

In the context of retail transaction scenarios from a centralized CBDC architecture, various approaches and standards aim to ensure efficient and secure processing of payments, and may still apply. One notable standard is the Payment Services Directive 2 (PSD2), a regulation within the European Union that has introduced transformative changes to payment services. Under PSD2, third-party providers are granted access to account information and Payment Initiation Services (PIS), enhancing competition and innovation in the financial sector.

This approach enables consumers to authorize these third parties to initiate payments on their behalf, creating new avenues for digital payments and transactions. This is centralized, as licensed third-party providers are granted access, and are subject to strong regulatory reporting requirements.

Additionally, the ISO 20022[45] messaging standard is gaining traction globally, offering a comprehensive data model for financial messages. This standard enhances the richness and quality of transaction information, leading to improved interoperability and streamlined communication between financial institutions. With its extensive scope, ISO 20022 can be applied to various transaction processing scenarios, from retail to wholesale payments, fostering consistency and efficiency in financial messaging.

In addition to financial institutions like banks supporting these standards for extensive interoperability, trusted and licensed intermediaries can provide additional services such as seamless transactions, supporting card and offline payments, and providing secure implementations of services to fill requirements in the ecosystem.

4.5.2.2 Decentralized

In the scope of decentralized payment systems, many regulations related to protection against criminal activities and towards anti-money laundering, as described in the previous section. However, developments of standards in decentralized payment systems such as blockchain payments are actively in development, with technology-agnostic standards being introduced primarily through the industry and academia. Standards institutes and Research organizations leading these developments include IEEE (the Institute of Electrical and Electronics Engineers), the W3C (World Wide Web Consortium), ETSI (European Telecommunications Standards Institute), and many others based outside the European Union. It is also observed that many of these standards have significant overlap, and there is not sufficient collaboration across standards. A comprehensive guide to all the diverse standards related to blockchain technologies, cryptocurrencies and ledger-based payments is beyond the scope of this report, but we describe a few of these standards to provide a basic introduction to the domain.

IEEE Standard 2143.1-2020[46] outlines the universal procedure for cryptocurrency payments, providing directives towards how consumers buy products or services with digital currency and merchants receive fiat currency in exchange. The standard covers various components, including cryptocurrency payment operators, consumer ownership of cryptocurrency, merchant access to payment platforms, banks, and cryptocurrency exchanges.

ETSI has introduced GS PDL 011[47], as part of a series focusing on the implementation of permissioned distributed ledgers (PDL). These specifications aim to capitalize on the operational and security advantages inherent in decentralized transaction recording, while simultaneously ensuring cost-effectiveness and scalability. The framework outlined by ETSI's Industry Specification Group for PDL (ISG PDL)[48] facilitates secure smart contracts, fostering transparency, fraud prevention, customizable domains, and data privacy preservation across diverse sectors, from healthcare and government to private individuals, and potentially smart-contract observability over CBDCs.

45 ISO 20022 Financial Messaging standard
46 ISO 2143.1-2020 – Standard for General Process of Cryptocurrency Payment
47 ETSI GS PDL 011 v2.1.1 - Specifications for Requirements of Smart Contracts' architecture and security
48 ETSI ISG PDL

Blockchain Research

A valid architecture design, supported by various pilot programs worldwide, is a private blockchain maintained and supported by the ECB. In the wild, cryptocurrencies like Ethereum have pioneered the usage of smart contracts and programmable tokens, integrating privacy-enhancing technologies while still supporting auditing and regulatory compliance in various ways, and the technology and the surrounding ecosystem are reasonably mature. A centrally-mandated and regulated cryptocurrency has a greater chance of meeting the ideals and principles of the Eurosystem towards a Digital Euro.[49]

49 Blockchain | TNO

4.5.3 Impact

4.5.3.1 Inclusion and Openness

Centralized systems
- Facilitate faster implementation and updates, potentially allowing for quicker inclusion of new features or technologies to meet evolving user needs.
- Tend to have stricter regulatory oversight, which can provide a sense of security for users and foster trust in the digital currency ecosystem.
- May face challenges in ensuring openness and fair access, potentially leading to exclusion or discrimination, as control rests with a central authority.
- Could limit innovation and competition due to a single governing body's control over the technology stack.

Decentralized systems
- Enable a more open and inclusive digital currency ecosystem, as they rely on distributed networks, reducing the risk of monopolistic control.
- Promote innovation and competition, allowing various parties to develop applications and services that can enhance the digital currency ecosystem.
- May face challenges in achieving consensus among network participants, potentially leading to delays or disputes in system updates.
- Require users to take more responsibility for their security, potentially excluding those who are less tech-savvy or lack access to the necessary resources.

4.5.3.2 Financial Security

Centralized systems
- Offer the potential for robust security measures, benefiting from economies of scale and centralized expertise in cybersecurity.
- Are susceptible to large-scale breaches, posing significant risks to financial security if the central system is compromised.
- Can implement strict fraud detection and prevention mechanisms to protect user assets.
- May be attractive targets for cyberattacks due to the concentration of valuable data in one location.

Decentralized systems
- Distribute data across a network, making it harder for attackers to compromise the entire system in one go, enhancing financial security.
- Rely on cryptographic principles and decentralized consensus mechanisms to protect transactions and user assets.
- Require users to have a higher degree of personal responsibility for securing their assets, which can be both an advantage and a challenge.
- May face security vulnerabilities in smart contracts or the underlying blockchain technology, which can impact user financial security.

4.5.3.3 User Trust (including privacy)

Centralized systems
- Can inspire trust in users through established customer support and dispute resolution processes.
- May erode trust if the central authority mishandles user data or engages in unethical practices.

- Offer a sense of familiarity and reliability, especially for individuals accustomed to traditional banking systems.
- Depend heavily on the reputation and credibility of the central authority to maintain user trust.

Decentralized systems

- Foster trust through (partial or full) transparency, as users and or trusted third party auditors may verify transactions on a public or hybrid-distributed ledger.
- Place trust in applied and exhaustively audited cryptographic principles rather than policies and centralized entities, potentially appealing to those who value decentralization.
- May face challenges in providing support and dispute resolution mechanisms, potentially leading to trust issues if users encounter problems.
- Depend on the integrity of the network's consensus mechanisms to maintain trust, which can be affected by the behavior of network participants.

4.6 Settlement

4.6.1 Description

As the second aspect of a financial transaction, the settlement of a financial transaction refers to the final and irrevocable transfer of ownership and funds between the parties involved in the transaction. This process plays a fundamental role in the functioning of modern financial systems, ensuring that transactions are executed smoothly and securely, while also providing legal and financial certainty to all parties involved.

Settlement involves two key components. Firstly, it involves the finality of the transaction, meaning that once it is settled, the transaction cannot be reversed or canceled without the consent of all involved parties. This characteristic provides a high level of security and trust in the transaction process, as participants can be confident that once the settlement occurs, the transaction is legally binding and cannot be unwound without mutual agreement.

Settlement also includes the reconciliation of the transaction details and confirmation that all contractual obligations have been met. This process ensures that both the payer and the payee have fulfilled their respective responsibilities in the transaction, such as delivering goods or services in exchange for payment. It acts as a safeguard against fraud and helps maintain the integrity of the financial system.

In the context of the Digital Euro, centralized and decentralized CBDC architectures have different roles, but considering the nature of distributed ledgers, Settlement is not a technically intensive step in the process, and should not have a significant impact on the end-users, as it is largely a process between financial intermediaries.

4.6.2 Supporting Technology and Standards

4.6.2.1 Centralized

Centralized CBDCs may or may not have intermediaries – depending on how centralized the architecture design is.

In a highly centralized design, these consequences are similar to those of a traditional non-CBDC currency, and end-users are insulated from the process.

In a more mixed-architecture with trusted nodes still managed by a central authority, transactions do not involve intermediaries, and no settlement step is required.

4.6.2.2 Decentralized

As decentralized CBDCs are usually P2P, they do not involve intermediaries that require a settlement step, and thus influence upon end-users is minimal.

4.6.3 Impact

Since the role of technologies in Settlement of the Transaction Process Flow is minimal for most CBDCs, the impact of choosing such technology is minimal, and is largely similar to the impacts defined in the previous section towards the impacts of choosing technologies for Transaction Processing.

Conclusion

This report is intended to provide an introduction to the Digital Euro development landscape, and mentioning the current developments. It provides the initial architecture by the Digital Euro, and describes the possible technologies and standards that could be made in the context of one of the most fundamental process flow – the Transaction flow - in significant detail. Impacts for these technologies and standards are also described. We have identified the following key takeaways:

Key takeaways:

1. It is expected that the Self-Sovereign Identity (SSI) ecosystem is of vital importance for **the digital identity**. Based on recent regulation related to a European Digital Identity, such identities are increasingly being designed for various use-cases. SSI ecosystem concepts are compatible with both centralized and decentralized implementations of a CBDC.
2. Privacy-Enhancing Technologies (PETs) encompass a range of digital technologies wdesigned to protect sensitive information and safeguard the identities during the **transaction initiation** and **transaction processing** of the digital euro from malicious access.
3. **Settlement**, while a critical component ensuring finality and user trust in financial transactions, is generally not a technically intensive step in the process and technology choice has a minimal impact on end-users, whether in centralized or decentralized systems.
4. The **end-user adoption** depends on the impacts of the underlying technologies and standards that the Digital Euro will have, and should be considered for a successful roll out safeguarding citizens interest and concerns.
5. The choice between centralized and decentralized systems in digital currency ecosystems, which is the network of stakeholders and technologies enabling the creation, distribution, and use of a digital currency, is influenced by various factors, with user trust playing a significant role. Centralized systems may provide trust through standardized processes but raise **privacy concerns**, while decentralized systems empower users with greater control and transparency but can face challenges in building user trust due to their novelty and impact financial inclusion.
6. A **private blockchain** maintained by the ECB offers a promising path for achieving the Eurosystem's Digital Euro objectives in a decentralized manner with a strong focus on privacy and security, while supporting robust auditing and regulatory compliance.
7. The report provides a comprehensive overview of potential technologies and standards for the Digital Euro Transaction Process Flow. It underscores the importance of adopting a balanced approach and highlights that the **choice of technologies and standards**, whether centralized or decentralized, should be made **individually for each building block**, considering their respective advantages and impacts.

Contact

Authors

David Otto
Abhishek Mahadevan Raju

Review role

Freek Bomhof

Contact

David Otto
Consultant Innovation Strategy & Policy
TNO Vector

david.otto@tno.nl
+31 6 11 07 21 10
https://www.linkedin.com/in/dpotto/

TNO is an independent public research organisation. With over 4,000 specialists, we work together with entrepreneurs, scientists, policymakers, individuals, and society as a whole to create a safe, healthy, sustainable, and digitally connected society. Technological innovation can bring health and happiness to people and the planet. That is what drives us every day.

Acknowledgement

We want to thank the following experts for their feedback:
Freek Bomhof, Géraud Guilloud, Herman Pals, and Jean-Louis Roso

TNO 2024 R11044

tno.nl

TNO innovation for life