Download the latest version

Requirements for the success of a digital euro

Eduard de Jong

version 2—21/03/23
initially published—21/03/23

Abstract

The issuance of a digital currency by a central bank (CBDC) is foremost a political decision as it concerns the accessibility by the citizenry to the means of payment in a society. The technical solution to implement CBDC must follow the political objectives. This note presents the key political aspects to be considered and analyses risks, technical requirements and business perspectives of current proposals, in particular for the digital euro.

1 Introduction

The requirements for a digital euro, must be grounded on money as a social good. These requirements must be captured properly so that the resulting implementations will be widely accepted and will work as required to comply with EU law and policy. These requirements can be implemented with existing technology, but not with existing products that were built to meet different requirements. My observations here are from the perspective of an expert in this domain. I have over 30 years experience with the technology and the standards required to enable it.

There are three types of money, Bank Reserves, Commercial Bank Money, and Cash. Real world implementations of bank reserves and commercial bank money have already moved to the digital world. These are account-based systems that are easily and effectively implemented using standard software technology. Cash is different. It has unique requirements that cannot be met with ledgers and standard software. The role of CBDC is to fill the gap for cash in the digital realm.

	Cash	**Bank Reserves**	**Commercial Bank Money**
Physical	Notes and Coins	Paper Ledgers Legacy/Obsolete	Paper Ledgers Legacy/Obsolete
Digital	CBDC	Digital Ledgers	Digital Ledgers

A digital euro must be cash-like in order to succeed as a CBDC. To understand what this implies, we need to look at all aspects of what it means to be *like cash* in a digital world.

One of the primary roles for cash is for payment. The current absence of a CBDC has created a business opportunity for commercial enterprises to offer different forms of digital payment. While these may be suitable for a variety of commercial uses, they are not cash.

It may be appropriate for governments to create and manage citizen accounts for activities such as taxation, but these accounts are not cash.

Attempts to enhance these accounts with additional features will not turn them into cash.

Cash facilitates commerce because it can be used anywhere, anytime, without an intermediary. It is the role of government to insure that that the essential features of cash are delivered by the digital

euro in a form that aligns with all of the requirements of the EU.

Here are some of the specifics that need to be addressed by a digital euro.

2 Political aspects

Money is a public good. This overarching requirement has major implications for cash. Cash is, and should, be a primary form of payment. It is the money of last resort for the poor, for social outcasts, political dissidents, and other disenfranchised groups. To succeed, any implementation of a digital euro must meet the needs of the public.

- Privacy
- Accessibility
- Social justice
- Financial inclusion
- Oversight/AML

Privacy

Privacy protection must be by design. Only data that is not captured cannot be compromised.

The experience is clear: large, valuable datasets can be compromised. In the last decade, personal information has been exposed for over 1000 million people!

With modern cryptography, secure payments can be managed without including the identity of both parties in each transaction. Protecting privacy is an essential design requirement for digital payments, this means that the resulting data does not contain information that can be abused.

Both on the anti-government right and on the populistic left a lot of noise is being made on the claimed lack of privacy protection in the digital euro as currently proposed. In particular, a Big-Brother narrative is constructed with the ECB as actor for government spying to enable control. The technical design currently being discussed for the digital euro project make this narrative credible. How far can you trust the system to be private, if transactions might be revealed due to a technical failure, a corrupt administrator, or a change in government?

It is possible to operate a system with oversight, without also collecting and storing every detail.

Accessibility

Payments with a digital euro must be usable by every European citizen and enterprise.

One of the important benefits of a digital euro is the opportunity to improve accessibility. Personal digital devices to make a digital payment can be made available to anyone, e.g distributed via post offices and social services. They can be implemented with access enhancements such as larger typography and audio feedback, along with a wide range of input devices. Since populations with accessibility issues vary in size and needs, it is essential to require the system follow open standards so any organisation or group can develop and deploy fitting devices.

Having a secure hardware device for payments is essential to give the user true ownership of digital

money. This will require oversight and supply chain management for the devices. It is also important to make as much of the system as possible work with unsecured software to lower the cost and increase the flexibility of devices and networks that can used.

Social justice

Cash is for everyone, not just favoured groups and elites.

Physical cash plays an important role in social justice, placing day-to-day payments for goods within reach of everyone in society. While bank accounts and ledgers play a very large and important role in financial systems, they are subject to social manipulation. Outcast groups are denied accounts, political dissidents have payments blocked, and other injustices are enabled.

A Central Bank Digital Currency (CBDC) for the euro must provide cash-like resistance to political manipulation and deliver a payment system that works for everyone. This starts with privacy, and includes requirements for independence from centralised controls and 3rd parties who might be tempted to manipulate access, e.g by monetising it.

Financial inclusion

For individuals without access to accounts, cash is a lifeline.

The digital euro must fit in with the current banking systems and accounts, and, it must also work for situations and people that do not have access to banks and accounts. To achieve this, its technical design must allow direct distribution and use of digital euros.

There are always unbanked individuals, who nevertheless need access to funds and payment services to survive. A digital system can enable this and make life better for the individual, without the need for “on-boarding” or other hurdles. At the same time, the issuing central bank can retain overall control and oversight of the situation by enforcing policy within the system. With the right design, a digital euro can be a significant improvement over physical cash.

This type of inclusion is also important in situations that may arise due to natural disasters or infrastructure failures, temporarily rendering a larger population unbanked and unable to access their accounts.

Whatever the reason for these situations, the digital euro must function for these individuals at such times. A digital euro can be faster and easier in reaching the intended recipients than physical cash.

Oversight/AML

Visibility and controls, not Big Brother.

A cash-like CBDC must monitor the system for security and operational management, e.g. money velocity, volume, and unusual patterns. For this purpose the system implementation must provide the means to gather operational data.

The identity of the payer in every transaction is not required. Privacy can be absolute. Operational data can be obtained by monitoring received cash-like payments. This data set is sufficient to insure the correct operation of the system. Illegal activities such as money laundering, can be detected from the pattern of receipts. This is also appropriate for tax avoidance. Even this can be done while still protecting the payee identity by using pseudonymous identifiers. Regulators need to focus on the pattern of transactions to identify suspect activities.

Current AML regulations were introduced for accounts that know personal details of both parties involved in the transfer. The legal texts will need to be updated to focus on the pattern of receipts, sufficient to justify unmasking the participants.

3 Technology

Technology must meet the requirements for the Digital euro, not the other way around.

In order to deliver the key requirements for privacy, accessibility, social justice, and financial inclusion, the digital euro must be a cash-like system.

There are on-going discussions about an account-based digital euro. The current architecture and technical design from the ECB is for creating bank accounts for all European citizens. This design depends on commercial banks willing to act as intermediaries to authenticate users and forward the payment authorisation to the central bank maintaining the citizen's accounts. It also depends on third parties to provide the secure devices that give users control over spending. This may be a useful extension to bank accounts in the EU, but it is NOT a digital euro. It fails immediately on actually, convincingly, providing privacy, social justice, and financial inclusion.

Meeting these requirements requires a cash-like system that can function completely off-line with value held in true bearer payment instruments. Technology is available for electronic cash (e-cash)[1] that meets this requirement. E-cash provides inherent protection of payer privacy as no data is recorded of the person making the payment. It supports any type of payment both offline and online. An e-cash payment is between two parties, it is final there and then. No intermediaries are required. It can issued by any of the central banks in the euro system and securely provisioned to users by banks, social services or post offices. Development and deployment cost for an e-cash digital euro, as well as operational costs, will be significantly less than for an account based system with intermediating banks, large replicated data centres and hardened communication infrastructure.

There will be development costs to create the detailed requirements and to configure and test a system that meets them. Commercial off-the-shelf solutions are designed to capture fees and transaction details that could be monetised. The digital euro requires technology that protects the privacy of payments and minimises transaction costs so that payments can be free.

A system that implements direct peer-to-peer payments will protect privacy by design. Because payment is between two devices, higher payment volumes will not result in higher backend costs, as it will for any ledger or account-based system.

The core design must then be standardized and delivered through well-established open source licenses to enable the participation of a wide range of vendors. The operation of the digital euro must include testing and validation for critical system components.

Technical Dead Ends

- Account-based systems – While accounts are very capable systems, they do not meet the requirements for a cash-like digital euro.
- Distributed Ledger Technology (DLT) – Crypto currency systems like Bitcoin and Ethereum

1 More information on e-cash as digital euro can be found in https://eduard.dejongfrz.nl/papers/latest-kingwillreturn.pdf

have made extravagant promises for many things they are incapable of delivering. Payment and privacy are well known examples. None of these systems meets the core requirements for a digital euro. The loud, aggressive, and well-funded promotion of these technologies is a reflection of their culture, not their suitability for this purpose.

4 Risks

Failure of the digital euro project will have a political impact both on the EU internal position of the euro and on its the global standing. Several threats can be identified in the project to issue a digital euro:

1. Failure to be adopted or adopted in sufficient number by European citizens and enterprises.
    1. Poor adoption by users. The user experience must be positive and compare favourable to alternatives. This requires both careful implementation and testing, as well as messaging to support the project;
    2. Limited adoption by merchants. Their benefits must be greater than the direct, operational, and administrative costs;
    3. Poor adoption of offline payment. Enabling offline payment is a signature feature for digital payment. Experience from many decades shows that users need a lot of education to change their behaviour, even when it is in their best interest;
    4. A widely held perception that the privacy protection is insufficient, in particular in comparison to traditional cash payments where no personal data can be collected.

    A digital currency creates a classic "chicken and egg" problem. Both user and merchant acceptance is essential and neither can come first. This requires careful planning to ensure that "critical mass" is realised by techniques such as geographic sequencing or market segment enablement.
2. Failure to realise key objectives:
    1. Excluding the underbanked and socially weak from digital payments;
    2. Not reducing cost of payment for society;
    3. Privacy that is absolutely protected by a design based on strong principles;
    4. Poor environmental footprint;
3. The digital euro project as currently design is technically complex, it involves a large number of functional components that interact with each other and are operated by multiple parties.
    1. Cost overrun is rather common for large IT projects, as is initially underestimating the costs to make it politically acceptable
    2. Participating financial institutions claiming excess development expenses for integrating functional components, with leverage over the ECB as their collaboration in the project is essential for deployment and possible success.
    3. Failure for external funding to become available at the right level for the expected FinTech innovations to be able to be realised.
4. Large IT system are known to have security failures that may result in privacy protection violation, identity theft and fraud. Any such a breach will damage trust in the digital euro.
5. The current design enhances critical dependencies in the payment system by relying on availability of data communication that is to be provided by commercial entities.

Annex A to the 2020 report by experts from several central banks published by the BIS on the foundational principles and core features of CBDC presents a list of 14 essential questions that are strongly recommended to be answered for each concrete deployment of a CBDC. The ECB should provide answers to all of these questions based on the current proposal.

5 Legal

Compliance with applicable laws is a requirement.

As a technology expert, my only comment on the legal aspects of a digital euro is a reminder that the legal structure of the EU is the framework that the digital euro must fit within.

In this context, the extant legal framework gives the European Parliament a role in the usability of the euro, that is, specifically on the mentioned key design requirements, privacy, accessibility and financial inclusion.

If a potential technical solution does not meet these essential requirements it will fail.

6 Conclusion

The focus for a digital euro must be on a comprehensive set of requirements that will ensure the success of the project. Therefor technologies must be selected that can convincingly meet every aspect of these requirements.

From the set of requirements summarised in this document, we can see that an account-based technical solution fails in essential areas. The projects working on accounts must either be stopped, or re-framed as what they are: enhancement to existing account systems.

The digital euro efforts must focus on the gap in the monetary system: real digital cash with an offline store of monetary value and with immediate settlement of all payments.

Table of Contents