Introduction

In recent years, the European Central Bank (ECB) has increased its efforts in exploring the possibility of realising its own Central Bank Digital Currency (CDBC), the 'digital Euro'. A report published by ECB in 2020 and a keynote speech by Fabio Panetta, member of the Executive Board of the ECB in 2022, outline various reasons for the desirability, necessity even, of such a project [BRON] [BRON].

Perhaps the most urgent reason to warrant a digital Euro is the rise of digital payments and corresponding decline of cash usage. As Panetta mentioned in his keynote speech, cash is currently the only publicly accessible form of sovereign money. Digital payments are made using services provided by private and/or foreign actors - foreign referring to outside of the Eurozone - using money that is a liability of the respective actor and not a claim on a European central bank. Panetta fears that, without a publicly available and ECB-regulated digital payment system, European public money will become 'marginalised'; replaced by other forms of currency. This potential 'currency substitution', as the aforementioned ECB report calls it, could reduce effectiveness of ECB's monetary policy, harm market competition, and finally even threaten the European Union's strategic independence. The private and/or foreign actors that are largely responsible for the fear or currency substitution are large corporations, big tech, and foreign central banks if they decide to deploy a CBDC and make it available to European citizens.

In order to compete with these parties and make its CBDC attractive for mass adoption, the ECB has enumerated many requirements and wishes for its CBDC [BRON]. In the keynote speech, Panetta highlighted the necessity of digital Euros to be anchored to physical Euros in terms of value. In the same speech, the motto "pay anywhere, pay easily, pay safely" was coined [BRON]. Moreover, the ECB report reflects the ECB's wishes for its CBDC to also enjoy beneficial cash-like features, such as being protective of citizens' privacy, being spendable in an offline setting, and being able to be remunerated at varying interest rates. For a full specification of the ECB's requirements and wishes for its CBDC, we refer the reader to an ECB report on the subject [BRON].

Some of the demands and wishes mentioned by the report are difficult to realise individually and perhaps not even unifiable together, spawning multiple analyses for different scenarios and use cases. This research focuses on a scenario that attempts to closely resemble cash usage; physical Euros are mimicked by digital units of fixed, undivisible value ('tokens') and emphasis is placed on researching their spendability in an offline setting. Due to technical limitations however, some design choices were made that do not fall in line with the anonymity and decentralisation of cash usage, such as the choice for a centralised validation process instead of peer-to-peer. Please refer to Section ? For further elaboration. The transaction system that inspired this research was introduced in a work by Blokzijl [BRON] and modified for this scenario. This research contributes (1) an improvement in transaction throughput and scalability compared to Blokzijl's system (2) a performance analysis of various bottlenecks in the system to highlight its weaknesses and potential upper performance bounds and (3) a fully rewritten and software-tested reference implementation.

Public money for the digital era: towards a digital euro - F. Panetta
Report on a digital euro - European Central Bank

Problem Description

Ideally, a cash-like CBDC should be fully decentralised, spendable offline, and have immediate deterministic transaction finality like cash. However, to the best of our knowledge no system exists that combines these properties, which raises questions about how far a CBDC should and could go to imitate cash. Blokzijl's system and the system highlighted in this research face similar difficulties in that regard. This research has inherited some design decisions of Blokzijl's system; we consider this acceptable within the limited scope of this research, the scope of Blokzijl's system upon which this research was inspired, and the broader context of the given scenario.

An important deviation between the systems is that Blokzijl uses a balance-based approach as opposed to token-based in this research. A token-based system requires generation of tokens and a modified transaction protocol. The token generation process is described in Section ? and the transaction protocol in Section ?. A major implication of a token-based system is that multiple tokens need to be sent per transaction, comparable to how cash payments often require multiple notes and coins.

However, the challenges presented to both systems are more similar than they are different. Both systems require their currencies to be 'stable', anchored to the price of the Euro. Blokzijl chose for a system where an exchange guarantees that 1 unit of their currency can at all times be bought or sold for 1 Euro. This is a commonly used practice to keep the value of an asset stable compared to another asset and it requires every unit of currency to be collateralized by 1 Euro. We saw no major limitations with regard to this approach in the scope of this research, and decided to not further concern ourselves with exchanging currency.

Another challenge that both systems face pertains to the ECB's desire for its CBDC to be spendable offline, without an internet connection to the rest of the network. In both decentralised and offline transaction systems it is non-trivial to verify whether parties still own the funds they want to spend and have not spent them before. We assume the reader to be familiar with this so-called 'double spending problem' [BRON]. To mitigate the impact of the double spending problem, Blokzijl's system leans on one or more validators to verify balances. These validators are trusted parties in the network, and thus balance validation is not peer-to-peer but a centralised process. We opted for a validation system comparable to Blokzijl's; providing near-immediate finality and scalability at the cost of having to trust the network's central nodes. Different from Blokzijl however, validating nodes keep track of individual tokens rather than account balances, because this research implements a token-based system.

If validators are unreachable, Blokzijl's system allows transactions to be made in a peer-to-peer fashion, deferring finality until the proper validator is available again. In this period during which the system is offline, double spending can occur and can only be detected afterwards during the validation process. Though not ideal, it is in line with the design principles of Trustchain, the framework upon which Blokzijl's implementation was built, which also guarantees fraud detection but not prevention [BRON]. This research adheres to the same principles with regard to double spending.

From measurements it became apparent that Blokzijl's system's transaction throughput was not high enough to facilitate the needs of the Eurozone. Transactions were measured to be around ?, as opposed to for instance the VISA system that is capable of processing 24000 transactions per second [BRON] or Alipay that can process 544000 transactions per second [BRON]. It is worth noting that the scale of these systems is massively larger than the evaluation done by Blokzijl, which results in skewed measurements. The evaluation Section (Section ?) takes care to fairly compare Blokzijl's system with this work.

https://en.wikipedia.org/wiki/Double-spending
https://research.tudelft.nl/en/publications/trustchain-a-sybil-resistant-scalable-blockchain-2
https://usa.visa.com/run-your-business/small-business-tools/retail.html
https://www.scmp.com/tech/e-commerce/article/3038539/how-alibaba-powered-billions-transactions-singles-day-zero-downtime?module=perpetual_scroll_0&pgtype=article&campaign=3038539