

Problem Description

Leon Kempen

November 2023

1 Direction

The main direction of the thesis would be to create an offline alternative to the existing physical cash and online payment systems, providing anonymity and untraceability for its users. Incorporating a reliable offline payment system would make the current financial system more resilient and robust. Moreover, when the value-issuing (gold/CBCD) party is not a public bank, it could act as a competitor of the public banks, forcing them to be more attractive by, for example, raising their interest rates.

2 Focus

The thesis will focus on (digital) offline value transfer, albeit gold or CBDC tokens. Preferably, a token of value is transferable between different participants in the network without contacting the party that issues the tokens. As preventing double spending without trusted hardware is impossible, the act of double spending should be discoverable at a later stage.

To ensure that identities cannot be forged during the withdrawal process, it would be nice to integrate communication with an EBSI wallet during the process, when one would identify himself at the value issuing party.

3 Scope

The scope of the thesis would be to implement a prototype app with the functionality above implemented. The cryptographic principles would be taken from existing papers. The UI of the application can be based on existing bank applications. Other critical factors that should be considered are the security of the application and the scalability of the application. Since financial systems are regulated, laws and legality should also be considered. For example, when double spending results in debt creation, it would not be allowed, as this would result in unlimited debt creation, which is prohibited according to Dutch regulations.

4 **Ambition**

My ambition would be to create a prototype implementation of an offline value transferral scheme that could serve as an example of CBCDs. Potentially, this prototype can also be demonstrated during a workshop.