Experimental Design

January 15, 2024

1 Introduction

Both found offline e-cash schemes that provide transferability rely on extreme cryptographic protocols (malleable signatures, NIZK proofs and such) to provide transferability. However, if the DigiEuro were to be accepted by the public, those protocols might scare the masses. To prevent this, a solution that is less cryptographically extreme, and with that perhaps less efficient, might be preferred.

2 Design

Coin validity
If we have a representation of a coin, it should be verifiable by the receiver with the signature of the bank. However, this implies that the structure of the coin cannot change as a result of this would be that the signature would also change. Changing such a signature properly, such that it maintains its verifiable use-case requires complex cryptography and is thus unwanted.
The other option is to work with tags (serial number and double spending like Baldimtsi and Bauer) but solve the double spending prevention differently.
Serial nr. Tags (ST)
As the structure of the coin does not change, the identity of the spender should not be embedded in the coin but in the serial number tag. The tag is generated during the transaction when the (now) spender receives the token. That way, the coin is linked to the user before spending. This embedding should be done in a once-concealed, twice-revealed fashion.
This could be done with a method similar to Eslami, which is an ElGamel with a challenge (DLP). The result of that would be the double-spending tag (DS). After that, a new serial tag should be created by the spender and receiver.

The tags can be linked as follows:
- ST(i) refers to a hash of DS(i-1)
- DS(i-1) refers to a hash of ST(i-1)
- ST(0), generated by the bank and the first receiver and can be verified differently.