# A Swedish e-krona - technical considerations

October 2017

## Introduction

This document is a response to Riksbanken's request for input on how a technical solution for a Swedish e-krona could look like. The document describes a hybrid between a register-based and value-based solution, in accordance with the stated preference of Riksbanken. The different part of the solution could be implemented over several phases.

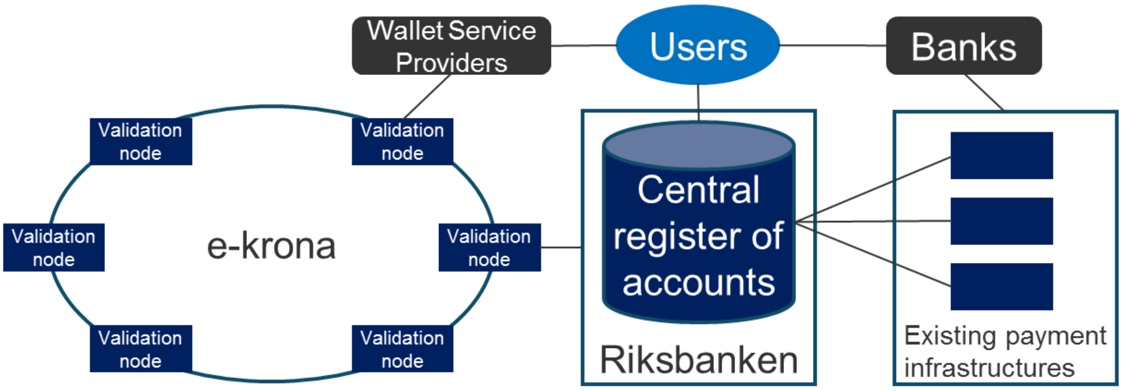
## Basic infrastructure

The infrastructure outline that we propose is based Distributed Ledger Technology (DLT), for two reasons:

- Firstly, we consider DLT to be the technology most likely to be used as the infrastructure layer of the next generation of digitalisation. The use of DLT for the e-krona will make it easier to build innovative solutions that automate administrative processes indirectly related to payments, thereby realising cost savings for the Swedish society as a whole - both the private and the public sector.
- Secondly, the use of DLT will make for a resilient e-krona infrastructure independent from existing payment infrastructures in Sweden.

The decentralised ledger may or may not be a traditional blockchain. If, for example, it is an important requirement to be able to prove individual payments in a court of law, a Merkle tree will provide for a much shorter path of authentication.

The exact design of the DLT should be closely aligned to the progress of the standardisation work done in ISO TC 307. Standards from ISO TC 307 are still a few years away, and an initial DLT solution will likely have to be replaced at some time, to promote interoperability with a greater eco-system of DLT solutions and ensure the encryption methods used are secure from quantum computing.



### Central bank money in a central register or as tokens

In accordance with the report from Riksbanken, it is assumed that money in the central bank is kept at accounts in the central register, and the DLT is therefore merely a transaction layer. However, we recommend that Riksbanken considers the possibility of registering the central bank money as tokens on the DLT. In this scenario, Riksbanken would ensure a sufficient money supply by making tokens available on the DLT, adding and removing tokens as needed. This would make the transaction processing independent from a central register, as users can buy and sell central bank money directly on the DLT. Besides the operational benefits, new monetary policy instruments could be introduced with the use of smart tokens. One example would be targeted monetary easing (“helicopter money”), aiming specific users and/or having specific spending requirements (timeperiod, spending purpose etc.) to ensure maximum impact.

### Validation of transactions

The DLT will consist of several permissioned validation nodes, most likely licensed by Riksbanken. All the validation nodes will be connected to the central register of accountholders. To reduce the transaction costs to a minimum, we recommend to consider using one validation node to compile transactions, do AML checks and generate blocks. This leader is selected randomly and secretly, and a few other validation nodes (also selected randomly and secretly) verify that the leader has complied with all rules. Both the leader and the verifiers use zero-knowledge proofs to prove their respective roles to the rest of the network.

### Privacy protection

It DLT should not contain any personal data or allow profiling of users based on the DLT alone. Each transaction will use a unique identifier for the payer and the payee. These identifiers are generated by the central register of accounts and will be single-blinded, so an identifier by itself will not reveal which account it is linked to. The first identifier for a user is generated when an account is first opened and communicated as a valid identifier the both the user and the validation nodes. Whenever a transaction is registered in the central register of accounts, a new identifier is generated the same way.

It will require access to the central register to match an account to the corresponding transactions. If further privacy-protection is desirable, the identifiers could be double-blinded, but that would require an intermediate broker and thereby increase transaction costs. In a double-blind scenario, no single entity will be able to do profiling of users on its own.

### Offline operations

It is possible that the users, the validation nodes or the central register become disconnected from the network. As there are multiple validation nodes, the network will continue to operate even if some the validation nodes go offline or are compromised. If a user is offline, the solution will function as a simple wallet, with restrictions to the amount that can be spend and restricted to be used for retail payments where the POS terminal can handle offline transactions.

If the central register of account is offline, other restrictions will apply. If, for example, Riksbanken sets an upper limit (maximum the deposited amount) on how much a user can spend while the central is register, this amount is registered in the DLT with each new identifier. With homomorphic encryption, it would be possible to do computation (check that the limit is not exceeded) without decrypting the upper limit. When the validation node acting as leader for a block cannot connect to the central register, offline mode is activated and the same identifier is then reused, with the upper limit restricting the allowed spending during the offline period. Re-using the identifiers is required to allow the DLT to operate independently from the central register during this period. The validating nodes acting as verifiers will naturally verify whether they themselves can connect to the central register, and offline mode is discontinued once connection is re-established.

During the offline period, the identifiers are pseudonymous, thereby reducing the privacy protection. Assuming the offline period is short, limited profiling will be possible. Concern for profiling could be further reduced by having payment amounts also homomorphic encrypted during offline mode. However, the use of homomorphic encryption will reduce the performance of the DLT during offline mode.

**Network resilience**

As the central register of account is the most vulnerable part of the network, it should have dedicated lines to most of the validation nodes. The validation nodes should also have dedicated lines to some of the other validation nodes, to improve resilience from network attacks. A fully dedicated network is not required, but it should be prohibitively expensive for an attacker to cut off a substantial part of the validation nodes. A cluster analysis of the network is recommended.

**Implementation in multiple phases**

Stepwise implementation could start with a simple wallet solution – similar to existing wallet solutions, just with central bank money. The next step would be to add the DLT infrastructure to expand the use cases, and the central register with accounts could the added at a later stage.