E-krona pilot
Phase 1

SVERIGES RIKSBANK

April 2021

Table of contents

1 Why an e-krona?

The usage of cash in Sweden is declining. This is partly due to technological developments, which have given us several digital payment services. The Riksbank sees potential problems arising from the decline in cash and is therefore running a project to investigate the possibility of producing a digital complement to cash, which we call an e-krona. This report describes in brief the technical solution tested in the first phase of the e-krona pilot project, and the legal analyses of the solution. There is also an account of the overall lessons learned from the project and the next step in the work. However, there has so far been no decision on whether to issue an e-krona or on how the e-krona would be designed and which technology would be used.

The Riksbank is entrusted with the task of promoting a safe and efficient payment mechanism and since 1904 has had a monopoly on issuing Swedish banknotes. Cash is currently the only money issued by central banks available to the general public.[1] However, technological developments have meant that physical cash is more seldom used while digital payment services are becoming increasingly popular. When cash has to take a back-seat in favour of the private financial agents' digital services, this means that the Riksbank's direct role on the payments market is reduced. The Riksbank may then find it more difficult to fulfil its task of promoting a safe and efficient payment system available to all parts of society. Since 2017, the Riksbank has therefore been working on investigating what role the Riksbank should play in an increasingly digitalised world, and whether there may be reason for the Riksbank to produce a digital supplement to physical cash, an 'e-krona'.

The Riksbank's e-krona pilot

In 2019, the Riksbank established the e-krona pilot division, with the task of increasing the Riksbank's knowledge of how a potential e-krona could be designed, by producing proposals for a technical solution and investigating regulatory issues regarding an e-krona. In February 2020, following a public procurement procedure, the Riksbank signed an agreement with Accenture in the role as supplier of the technical solution tested by the e-krona pilot. The technical pilot solution that is developed in a closed test environment should not be interpreted as the solution the Riksbank has chosen for a potential e-krona, but as the method we have chosen as a concrete, possible, technical solution for analysing policy issues, technical issues, security issues and legal issues pertaining to a potential e-krona.

[1] See the Sveriges Riksbank Act (1988:1385) Chapter 5, Section 1 and Chapter 6, Section 7. There is currently digital central bank money in the Riksbank's settlement system, RIX, but this is only accessible to participants in the system, such as banks.

2 Tested technical solution during the first phase of the e-krona pilot

The e-krona in the technical solution tested in phase 1 of the e-krona pilot is token-based in a distributed network based on blockchain technology. Having a token based e-krona, which can only be created by the Riksbank, gives it certain attributes similar to physical cash. One such attribute is the possibility to store tokens locally with the end-user, which differs from the digital money we store in accounts today, and this creates alternatives for how the solution could be implemented. The e-krona network developed during the first phase, and which is described below, has been developed in a defined test environment where important parts such as participants, liquidity supply and end-users have been simulated.

2.1 E-krona designed as a token

The Swedish krona can be designed in different ways. The krona can have a physical form and comprise banknotes and coins that the holder can use by being physically in possession of them. The krona can also be in an electronic form, such as the money we have in bank accounts, where holders identify themselves to prove their right to use the money in the account. The e-krona in the technical solution that the e-krona pilot is testing is designed as a *token*, which means that it is a uniquely identifiable digital unit of value with the attribute that it can bear the value of Swedish krona. This does not have any great significance for how the e-krona appears to the end-user; the e-krona is similar to today's digital money, where you see the balance of your holding of e-krona and not one or more unique digital units of value. However, the e-krona's technical features create new possibilities that are worth further description and explanation.

The fact that the e-krona has the form of a token means that it shares a number of attributes with the physical banknotes, but also that it differs from them in some important aspects. As with banknotes, it is only the Riksbank that can create and issue e-krona. In purely technical terms, the e-krona is governed by a certificate showing that it is issued by the Riksbank, and as with banknotes the state is thus guarantor of the value of the e-krona. Each token also carries a specific value, but while banknotes have given denominations, the value of a token can vary. Like banknotes, each token is also uniquely identifiable, and the *e-kronor* it holds can be traced to the Riksbank as sole issuer.[2]

[2] Please note that with regard to the different forms used here *e-krona* denotes the singular and *e-kronor* the plural form (1 *e-krona* but 2 *e-kronor*)

The fact that the e-krona is digital in the form of tokens also differentiates it from physical cash. To obtain access to and make payments with the e-krona, it is necessary to have a digital wallet linked to a payment instrument in the form of a mobile app or a card, for instance. Unlike cash that can be used between people without technical aids and without the involvement of a third party, payments in e-krona require that the payer can communicate with the e-krona network. This communication takes place through participants in the network, for instance, banks and payment service providers.

Another important technical difference is that a token can only be used once. Each transaction with e-kronor means that the token used is registered as consumed and the e-kronor included in the transaction gain new representation in the form of a new token for the recipient and if necessary, a new token with the change is returned to the payer. The total amount of e-kronor in circulation that can be traced to the Riksbank will remain the same, but the e-kronor will be represented by new tokens.

However, a fundamental principle is that the Swedish krona always has the same value, regardless of whether it is in the form of physical cash issued by the Riksbank, an account balance with a private actor or a digital e-krona issued by the Riksbank. The exchange from one to another shall always be on a one-to-one basis.

2.2 Distribution model similar to current model for cash

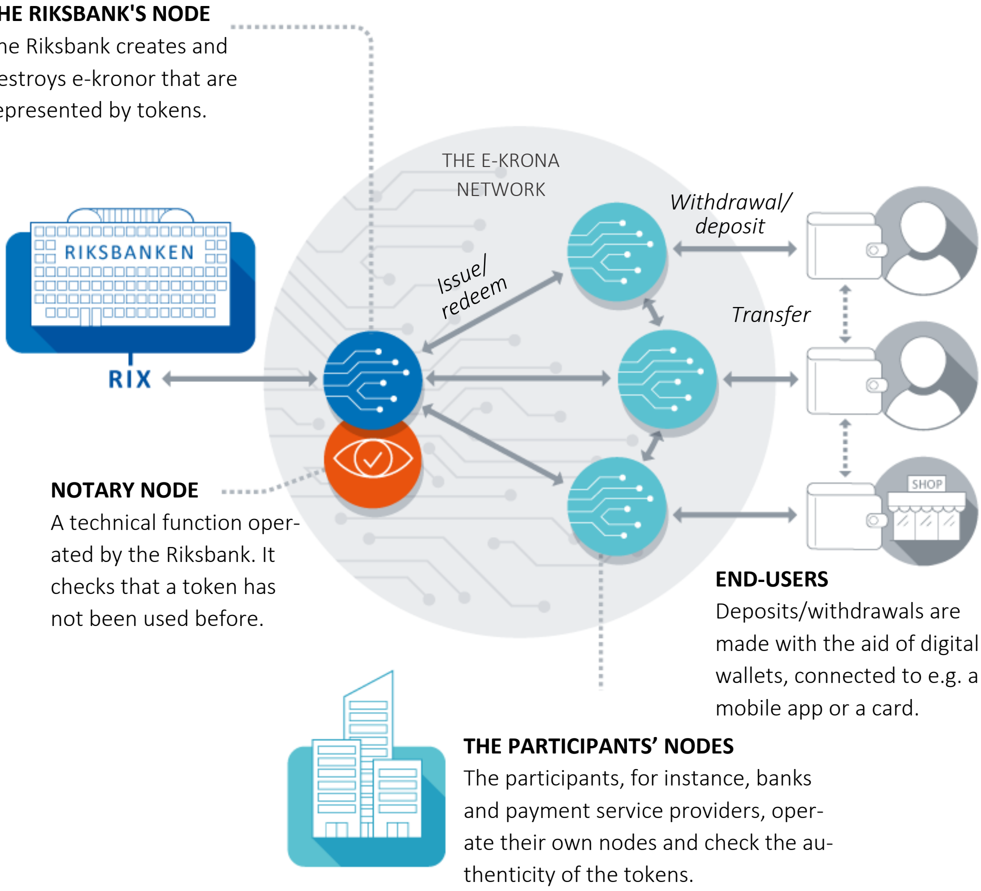
The distribution model in the e-krona pilot solution is reminiscent of how physical cash is distributed today. Physical cash requires for natural reasons a logistics model with longer lead times than the digital e-kronor, but from the perspective of roles and responsibilities there are clear similarities.

One such similarity is that only the Riksbank can create and destroy e-kronor. Another is that the Riksbank has a relationship with the distributors of the e-krona, known in the e-krona network as participants, who in turn have a relationship with the general public as end-users. Participants in the e-krona network run their own nodes, from which they can request that e-kronor are issued by the Riksbank in exchange for debiting their accounts in the Riksbank's settlement system, RIX. The e-kronor are then created by the Riksbank's node in the network and distributed to the participants' nodes in the network. The participants can then store e-kronor digitally in so-called participant vaults for further distribution to end-users. The participants offer the end-users the opportunity to exchange holdings in their payment accounts for e-kronor, via a digital wallet connected to a payment instrument, such as a mobile app or a card. This process is reminiscent of how one exchanges holdings in accounts for cash when making a withdrawal from an ATM, but instead of exchanging for physical cash, one exchanges for e-kronor, which are stored digitally. The e-kronor can then be used for transactions and, if desired, the user can exchange them back for holdings in their payment account via their participant, for instance, their bank. The participant can in turn redeem the e-kronor at the Riksbank, which will destroy them and credit the participant's account in RIX.

The e-krona network where the e-kronor circulate is based on the company R3’s Corda platform, which is a type of blockchain platform. The network is a decentralised private network (this technology is usually called DLT *Distributed Ledger Technology*), where the Riksbank as owner determines who may join as participant. The fact that the network is decentralised means that the transactions using e-kronor are registered with the participants in the network involved in the transaction, instead of in a central database. The participants, for instance, banks and payment services providers, run their own nodes in the network and thus have the possibility to request the issue of e-kronor and to exchange them, distribute them and to execute and receive transactions on behalf of end-users connected to them. The network is parallel and thus does not use the current existing infrastructures for payments using digital money, such as card networks and bank credit transfers. This means that payments within the network still could function when there are problems with the existing payment infrastructure. No new money is created in the e-krona network. Instead, the network is supplied with liquidity by the Riksbank's settlement system, RIX. In this aspect there is a dependence on an external system to create new e-kronor or withdraw e-kronor from the network.

Diagram 1. How the e-krona is distributed

Transactions within the network are made through nodes that are run by the Riksbank and selected participants.



THE RIKSBANK'S NODE
The Riksbank creates and destroys e-kronor that are represented by tokens.

NOTARY NODE
A technical function operated by the Riksbank. It checks that a token has not been used before.

END-USERS
Deposits/withdrawals are made with the aid of digital wallets, connected to e.g. a mobile app or a card.

THE PARTICIPANTS’ NODES
The participants, for instance, banks and payment service providers, operate their own nodes and check the authenticity of the tokens.

Diagram 1 shows a simplified chart of how the e-krona network and its participants are integrated and can communicate with one another and with end-users, how the e-krona network is supplied with liquidity and how transactions are executed. The transactions in the network are made in real time, and shall be available 24/7.

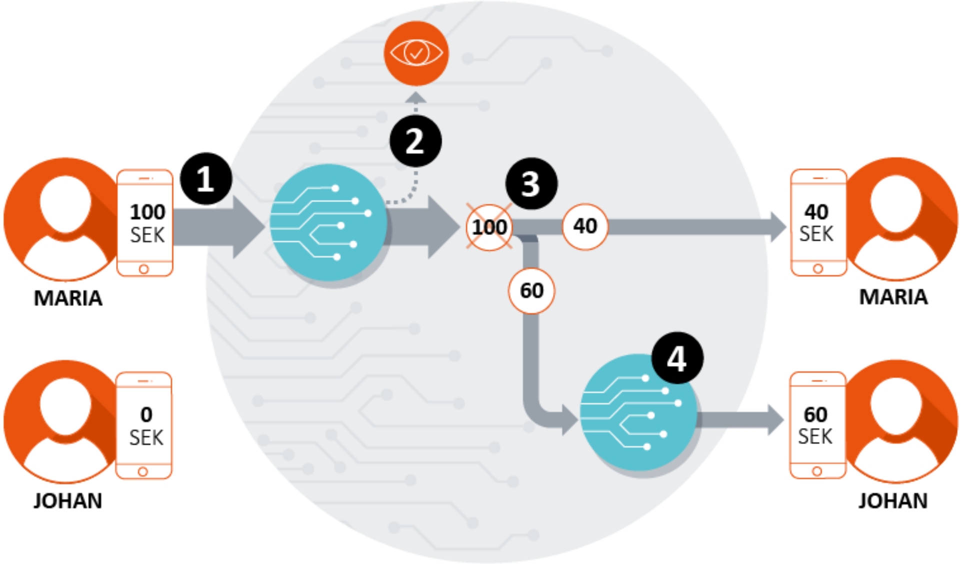
2.3 Authenticity of e-kronor verified in a transaction

When one has electronic money in an account, the balance on one's account is the result of ingoing and outgoing transactions in a controlled system (for instance, a bank's internal system). The account contains information on the holder of the account balance, but the money itself does not contain any other information than the balance on the account. With token-based e-kronor, on the other hand, the credibility of the actual e-kronor lies within themselves and in the information that can prove they are uniquely identifiable with a traceability to the Riksbank as issuer, as for cash. The e-krona network therefore needs to be able to validate and verify that the e-kronor used in a transaction are genuine.

To create security and trust in the means of payment of cash, banknotes and coins are designed so that they are easy for the recipient to recognise and difficult to counterfeit. With regard to e-kronor, their authenticity needs to be confirmed digitally within the e-krona network. As mentioned earlier, each token that represents a certain amount of e-kronor can only be used once. The task of ensuring the authenticity of the e-kronor is carried out by the participants' nodes by verifying that the e-kronor have a transaction history that can be traced to the Riksbank as the issuer. The control that the specific token used in a transaction is unconsumed, is carried out by a special control function in the network known as the notary node. The diagram below illustrates how a transaction in the network is made and what checks are made of which parties for the implementation during phase one of the e-krona pilot.

Diagram 2. How a transaction works

Maria wants to transfer 60 e-kronor to Johan. She has a token with 100 e-kronor in a digital safe at her participant.



1. Maria sends a request to her participant. The participant checks that there is sufficient funds for this transfer. Maria signs the transaction.
2. The notary node controls that Maria's token with 100 e-kronor has not been used previously. It is then registered as consumed and the transaction is approved.
3. Marias' participant creates a transaction with two new tokens (one with 40 and one with 60 e-kronor) and distributes them to Maria's safe and to Johan's participant.
4. Johan's participant verifies that that the token worth 60 e-kronor is genuine and stores it in his digital safe.

As the diagram shows, it is the sending participant that makes the first check when the transaction is initiated, to ensure the payer actually has the e-kronor they intend to send. The receiving participant validates that the e-kronor sent are genuine through a transaction chain that can be traced back to the Riksbank as issuer. The notary node, which is a technical function in the network run by the Riksbank, has only one task, which is to control that tokens used in a transaction have not been used before. Thus, the necessary checks that ensure the e-kronor are genuine and that a transaction can be implemented are made in the network. This process could be equated to a digital version of the controls we make ourselves when we receive cash. However, the controls in the digital network are made by the participants and the Riksbank, and not by the end-user as is the case with physical cash.

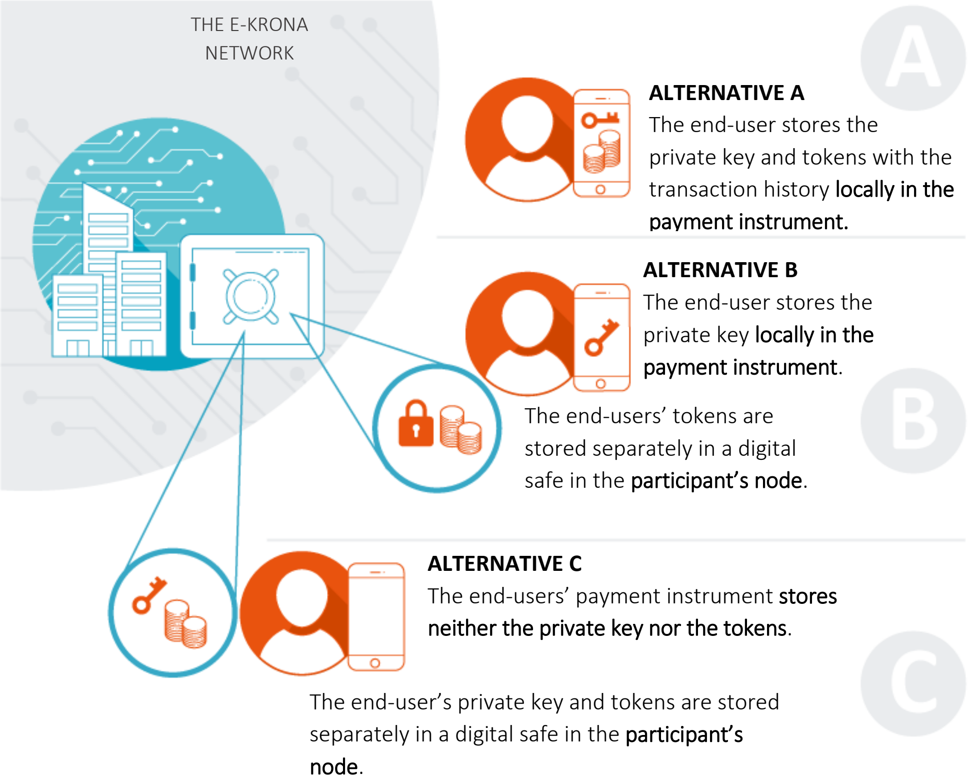
2.4 E-kronor can be stored in different ways

Various payment instruments such as a mobile app or a card make it possible to use the money we have in bank accounts, provided that we have access to an internet connection or a payment terminal. But the money is not stored locally and strictly tied to the specific instrument of payment; it is stored at a distance in the account system of those providing the accounts, such as banks.

As for banknotes stored in a physical wallet, it is possible to store the tokens and their accompanying information locally in a payment instrument. In this way, the money can only be used via the specific instrument where the money is stored. In phase one of the e-krona pilot, the tokens with e-kronor are not stored on the actual payment instrument, but in digital safe deposits in nodes at the participant to which the end-user is connected. However, the private key that gives the right to use the e-kronor is stored locally in the digital wallet connected to the payment instrument. This means that it is only possible to steer the money from that specific instrument. The technical solution for the e-krona pilot offers the opportunity to store e-kronor and their keys in a way that is more or less similar to physical cash or account balances according to the alternatives below:

Diagram 3. How e-kronor are stored

There are three alternatives for storing keys and tokens. In all three of them, the participants' own e-kronor are stored in its node in a digital vault.


THE E-KRONA NETWORK
A
ALTERNATIVE A
The end-user stores the private key and tokens with the transaction history locally in the payment instrument.
ALTERNATIVE B
The end-user stores the private key locally in the payment instrument.
The end-users' tokens are stored separately in a digital safe in the participant's node.
B
ALTERNATIVE C
The end-users' payment instrument stores neither the private key nor the tokens.
The end-user's private key and tokens are stored separately in a digital safe in the participant's node.
C

A. The tokens and the accompanying information of the e-kronor and their transaction history are stored locally in a specific payment instrument, together with the private key that is required to use the e-kronor. This is the most cash-like alternative. The storage gives the user exclusive control over the e-kronor connected to the payment instrument. The storage of e-kronor, their transaction history, and the ability to validate the authenticity of the e-kronor, described in diagram two, require a high level of technical capacity in the local payment instruments in the form of a mobile app or a card. This also means that, like cash, if a payment instrument containing money and keys is lost or damaged, it is more difficult to get it back, unlike money stored in an account system. The exclusive control over the e-kronor also means that this solution is difficult to combine with day-to-day financial services, such as direct debit, as no one other than the end-user has the possibility to reach the e-kronor through the payment instrument.

B. Tokens with accompanying information on the e-kronor and their transaction history are stored in the network in the participant's node, in a digital safe separate from the participant's and other end-users' e-kronor. The key to these tokens is stored locally in the payment instrument, which gives the holder exclusive rights to execute transactions with the money from the payment instrument where the key is stored. As mentioned above, this is the version tested in phase one of the e-krona pilot. The solution with a locally-stored key that gives the end-user exclusive rights to the e-kronor is also difficult to combine with day-to-day financial services such as direct debit.

C. Tokens with accompanying information on the e-kronor and their transaction history, together with the key to use them are stored in the network in the participant's node, separate from the participant's and other end-users' e-kronor. This alternative is very similar to an account balance with a linked payment instrument. Storage of keys and e-kronor at the participant gives the participant the possibility to make payments at the request of the end-users. This type of solution therefore enables financial services like those we are used to today, such as several payment instruments connected to the same account, and direct debit. The model therefore also makes the least requirements of the local payment instrument with regard to the possibility to store and validate information.

3 Legal analysis of the solution tested

The legal analysis has been based on the technical solution for the first phase of the e-krona pilot. An analysis has been made of the means of payment currently available on the payment market to see whether the tested solution would fit into any of the asset types that exist today, or whether a new asset type is needed. Further, we have looked at how this technical solution would relate to the anti-money laundering regulations.

3.1 E-krona as means of payment

In the legal analysis of the e-krona as a means of payment, we have compared the solution in phase one of the e-krona pilot to the means of payment we have today in the form of cash, account balances and electronic money. We have also compared it to cryptoassets. The type of blockchain and DLT technology used in the e-krona pilot is often linked to cryptoassets, as the technology had its major breakthrough with that type of asset. However, digital central bank money is not categorised as a cryptoasset. The reason for this is that central bank money has a state, a trusted actor, as issuer and that the state guarantees the value of the means of payment.

The question of digital central bank money that is available to the general public is relatively new and has only become relevant in recent years, both in Sweden and abroad. There is thus no legislation or any advisory example in this field. Issuing an e-krona would most probably require some new legislation, regardless of the model, design and technical solution used.

In the 1980s, certain financial instruments in Sweden were dematerialised. Prior to this, share certificates in physical form represented ownership in limited liability companies, but now it was no longer necessary for a physical object to be bearer of the economic rights. This development created a faster and more secure system for trading in financial instruments. Replacing or supplementing physical paper documents with a digital asset is thus not a new phenomenon.

E-krona compared with account balance

As illustrated in the description of the technical solution of phase one above, there are clear differences between the uniquely identifiable e-kronor distributed by participants in the e-krona network and the account balances with private actors. An account balance constitutes a claim on the private actor. In the current solution, the e-krona is stored separately in a digital safe deposit at the participant chosen by the end-user and shall not be regarded as an account balance.

E-krona compared with electronic money

Some institutions have the right to issue electronic money in accordance with the act on electronic money. In brief, electronic money can be described as a means of payment that can be issued by institutions that do not have the right to accept deposits and where the means are *prepaid*, which means that the institution may not use the means received. Electronic money may not bear interest, either. Issuance of an e-krona should be regarded as a step in the Riksbank's exercise of its role as public authority and the issuance of an e-krona will probably fall outside of the scope of the act on electronic money. Therefore this legislation does not give any further guidance for the design of the e-krona.

E-krona compared with cash

The only central bank money that is available to the general public at present is cash in the form of banknotes and coins. As already mentioned, there are some similarities with the tested type of solution for the e-krona that make a comparison with cash and the idea of the e-krona as a digital version of cash relevant. For example, e-kronor, like banknotes, are uniquely identifiable and can only be created by the Riksbank. The fact that the end-user, in the technical solution tested during phase one, has the exclusive right via the private key to use the e-kronor is also similar to our way of using physical cash. The similarities mean that one can argue that the e-krona belongs to the same asset type as cash, but in digital form instead of physical form. If an e-krona is to be mostly like cash, it will be difficult to apply interest to the e-krona as this would require an underlying claim.

An e-krona that is represented by tokens differs to some extent from cash, as it is digital and requires technical aids, communication and participants who enable transactions. This means that the e-krona possibly should not be regarded as belonging to the same asset type as cash, but should rather be seen as a new type of means of payment. This approach would probably require more extensive amendments to the legislation than if one were to regard the e-krona as the same type of asset as cash, but the advantage is that the legislation could be formulated in a way that suits the e-krona and its specific needs in a more appropriate manner.

3.2 Money laundering

Businesses that supply digital money and payment services are subject to the act on measures against money laundering and terrorist financing. This means that the institutions are obliged to have knowledge of the customers (KYC) using their services, and also the possibility to trace their transactions. An e-krona would probably also be covered by these laws and regulations. The distribution model in the tested solution distances the Riksbank from contract relations with the end-users. Instead, the responsibility lie with the participants in the network who have the role of distributors and offer the possibility to hold e-kronor and execute transactions on behalf of the end-users. In this way, the Riksbank could maintain its present role as issuer of money and supplier of the payment infrastructure while the KYC checks and monitoring of transactions would remain with the distributor, as is currently the case.

Anonymous payments are only permitted to a limited extent according to the current anti-money laundering legislation, and only smaller amounts can be transferred anonymously at present. Accounts may not be anonymous pursuant to current legislation, which should be borne in mind when discussing potential anonymous e-kronor. It is possible that there may be anonymous e-kronor, but they would have a very limited area of use.

4 Lessons learned

The technical solution that has been tested in the e-krona pilot project has resulted in a network where token-based e-kronor can be used for transactions in accordance with the distribution model described above. However, the solution based on DLT and tokens is a new technology that has not been tested before, and further investigation is needed to see whether it can manage retail payments at the scale and fulfil the requirements of digital central bank money. The potential advantages of the technology with regard to establishing a new parallel system for payments for increased robustness and the alternative possibilities for off-line payments offered by the local storage are also areas that need further investigation.

4.1 New technology that needs further investigation

The technical solution tested in the e-krona pilot is new technology for issuing digital units of value and managing retail payments on the scale and with the safety required by a digital krona issued by the Riksbank. The technology means that the e-kronor are similar to physical cash to the extent that one can trace their issue to the Riksbank and also because they are uniquely identifiable. However, this traceability requires that the network can follow how an issued e-krona has been used in the transactions leading up to the latest transaction. This raises a number of questions, for instance, how the technology can fulfil the banking secrecy requirements when making digital payments, at the same time as the solution requires that a chain of previous transactions needs verification to ensure the authenticity of the means of payment.

There are also challenges with regard to performance of a large scale retail payments system with a technology based on DLT and tokens. Each transaction in the tested solution requires that the history back to the Riksbank as issuer of e-kronor can be validated, and that the notary node controls that the tokens to be used have not been previously consumed. New tokens containing e-kronor are also created in the transaction. This process is information-intensive and requires a high level of performance. For instance, it must be possible to manage long chains of underlying transactions and situations where several actors or users at the same time request that a token containing a large amount of e-kronor should be divided into several tokens containing smaller amounts. The solution tested in phase one of the e-krona pilot has met the performance requirements made in the public procurement. But this has taken place in a limited test environment and the new technology's capacity to manage retail payments on a large scale needs to be investigated and tested further.

4.2 Local storage of keys and tokens and off-line payments

The way that keys and money should be stored with an e-krona should ultimately be determined by which functions are given priority in the e-krona. One question that has been raised as important for an e-krona is the possibility to pay off-line, and different ways of storing keys and tokens would provide different possibilities.[3] During phase one of the e-krona pilot, the off-line functionality has not been tested, but below follows a description of how the solution is intended to function with regard to off-line payments.

If keys and tokens are stored locally, in accordance with alternative A above, it should be possible to pay in the off-line position: the payer and the recipient should be able to execute a transaction and even validate that the locally-stored e-kronor are genuine when the recipient accepts the transaction. This means that the validation made by the participant in diagram 2 is carried out locally in the end-user's payment instrument. But it would not be possible to settle the transaction, that is, make the payment final, in the off-line position as the notary node in the network must first check that the tokens have not been used before. The final verification and settlement can thus only be carried out when one of the parties is on-line again. This type of solution could nevertheless offer an alternative for payments off-line, where the token is actually moved between the payer and the recipient, compared with today's off-line payments that are only possible via credit through certain card issuers.

The Riksbank has not tested the off-line solution yet, and nor has it yet investigated how a digital means of payment can function safely both on-line and off-line. The Riksbank therefore intends to continue investigating this issue. The fact that keys and tokens are stored locally in the payment instrument does mean, however, that vulnerability increases, as both of these can be lost in the same way as cash that is stored in a physical wallet. It is still uncertain to what extent it would be possible to retrieve the locally-stored money and how complicated the process would be if one were to break or lose the payment instrument. Another challenge is the technical ability of local payment instrument to validate off-line payments. This will also be investigated further.

However, as mentioned above, a solution based on tokens does not require that one stores keys and tokens locally. It is possible to manage keys and tokens in a way that is more or less reminiscent of how we store our digital money in accounts today.

4.3 Token model with balance cap and interest

The potential effects of a digital central bank currency on financial stability are a question often raised in the debate on CBDCs (*Central Bank Digital Currencies*). The possibility to control the supply and demand through a balance cap on wallets and interest on the e-krona is something that was tested during phase one. The technical solution with tokens as bearer of e-kronor is compatible with both a balance cap and either a positive or a negative interest rate. A positive interest rate would mean that the Riksbank pays interest in the form of new tokens with e-kronor to the holders of e-kronor

[3] Off-line is defined here as a lack of internet connection but access to electricity.

(the participant and end-user) via the participant, as shown in the distribution model above. However, one condition for a negative interest rate to be possible in the technical solution is that the keys to the tokens are not stored locally in the payment instrument (as in A and B in the explanations above). This is because local storage means that it is only the end-user with control over the specific payment instrument that has access to, and can execute, transactions with e-kronor. A negative interest rate would mean that, at the request of the Riksbank, a transaction with e-kronor corresponding to the interest is sent from the payment instrument to the Riksbank as recipient. As it cannot be assumed that the end-user is always on-line, accessible, has access to their payment instrument and executes transactions, negative interest is not compatible with local storage of e-kronor with exclusive control at the end user linked to the payment instrument. When storing keys and tokens with the participant, however, it is technically compatible. However, the compatibility of an interest-bearing e-krona, positive or negative, with a distribution model as tested in phase one, is a much broader question than the purely technical possibilities and limitations.

4.4 A parallel network makes the payment system more robust

One objective for the e-krona could be to increase resilience in the infrastructure for digital payments. The technical solution based on DLT and tokens means that one establishes an infrastructure that to a large extent could function in parallel to today's infrastructure for payments. It is therefore interesting to compare the two infrastructures with the starting point that the e-krona system shall be as independent and parallel as possible.

Factors that should be studied in a comparison include robustness, performance, communication and addressing of payments, and whether it is possible to settle payments. A more in-depth investigation is necessary to find out whether the new technology meets the requirements made regarding the infrastructure for payments today, and whether it is more or less appropriate than the already established solutions for retail payments with regard to bringing participants into the system, maintaining a high level of efficiency and low use of resources.

4.5 Legal issues

The legal analysis of the solution tested in phase one of the e-krona pilot has enabled us to come to certain conclusions.

E-krona and interest

If a token shall be regarded in legal terms as a *means of payment with an independent value*, that is, as cash-like, one might possibly use the legal principles applying to cash to the e-krona.

If interest were to be applied to the e-krona, one should instead consider constructing the e-krona as a claim. A *token* could then be classified as *a promissory note in digital* *form*. To simultaneously discuss *interest on an e-krona* and a *cash-like* e-krona as described in the section above should be avoided, as according to Swedish law, cash is probably a means of payment with an independent value. A *token* should not in itself prevent interest (positive and negative) being applied as long as the token is classified as some type of claim.

The state as guarantor for value of e-krona

The Riksbank/the state should be regarded as the guarantor of the e-krona, even when there are intermediaries in the e-krona system, as the Riksbank will be the sole issuer of the e-krona. Further investigation is needed as to whether the Riksbank, when it comes to the tested solution for e-krona, should in some specific cases undertake to redeem e-kronor directly from the general public.

The e-krona, banking secrecy and personal data

The technical solution that has been tested performs the authenticity check of tokens by transferring transaction history, which contains information about previous transactions, to the recipient. The information contained in an e-krona transaction about other customers and other participants than the customers and participants involved in the transaction must therefore be protected in such a way as to uphold banking secrecy and to avoid revealing personal data. The Riksbank is currently analysing to what extent the information stored in the transaction history can be regarded as information covered by banking secrecy and whether it comprises personal data.

5 Next step

The Riksbank has decided to extend the agreement with Accenture as technical supplier to continue testing the possibilities of the technical solution. The focus for phase 2 will be to include potential distributors of the e-krona as participants in the network in order to test how an integration with their internal systems could function with the e-krona network. The solution's ability to store tokens and their keys in different ways, and the capacity for off-line payments will also be investigated further. Continued testing of the solution's performance for retail payments will also be prioritised in phase 2.

The first phase of the e-krona pilot has resulted in an e-krona network based on R3's Corda blockchain platform in an isolated test environment. Central parts of the system have been simulated during the first year, such as liquidity supply via the Riksbank's settlement system, RIX, and participants in the network with the role of distributors of e-kronor. The simulated participants, end-users and payment instruments (mobile app, card and smart watch) and their functions have been tested by the Riksbank.

The Riksbank has decided to extend the agreement with Accenture for an additional year. The purpose of the extension is to further broaden and deepen knowledge at the Riksbank of how an issue of e-kronor could be realised, both technically and operationally. Through continued work on the tested technical solution, the Riksbank can continue to investigate and verify both the technical and the regulatory issues that are part of a digital central bank currency available to the general public. The work on the specific solution being tested in the e-krona pilot provides knowledge of this solution, but is also a starting point for comparisons with other types of solution for a potential e-krona. Below are some focus areas the Riksbank has decided to work with during phase two:

Integration with internal systems of potential participants

The participants in the network play a decisive role in this technical solution, both with regard to distribution of e-kronor to end-users and transactions in the network. During phase two the Riksbank therefore intends to allow market actors, who could potentially become participants in an e-krona network, to test this technical solution.

Develop off-line function

The possibility to make off-line payments is prioritised, as mentioned earlier, and will be investigated further. During phase one, we have only made a theoretical analysis of the possibilities of the solution. During phase two, an off-line solution with local storage of keys and tokens will be implemented and used in further tests that can provide knowledge of the possibilities and limitations of the solution.

Possibility to store keys and tokens in different ways

The technical solution offers different means of storing both the private key to the tokens and the tokens containing e-kronor. The different alternatives mentioned above have different advantages and disadvantages, which makes it interesting to evaluate the possibility of combining the different alternatives and using them for different purposes.

Develop the support for addressing payments

Ensuring the process of making payments in the network is easy is a necessary condition for an e-krona to be user-friendly. The design of the support for addressing payments will be investigated further in phase 2.

Evaluating and improving performance and scalability in the e-krona network

Which opportunities exist to attain sufficient performance and scalability for retail payments, is a question often discussed with regard to DLT and token-based solutions. During phase 2, this will be investigated and tested further.

Integration with existing point of sale terminals

The e-krona needs to be usable for payments in daily purchases at physical points of sale. For this to function, it is important that the e-krona is supported by the payment terminals that process other digital payments. This type of integration will be tested during phase 2.

Analysis of the e-krona network infrastructure

The aim of this focus area is to evaluate infrastructure, security aspects, communication within the network and out of the network, and division of responsibility among participants, and to identify potential network infrastructure.

SVERIGES RIKSBANK
Tel +46 8 - 787 00 00
registratorn@riksbank.se
www.riksbank.se

PRODUCTION SVERIGES RIKSBANK
ISSN ISSN. (on-line)