Riksbank e-krona project **October, 20 2017**

Massachusetts Institute of Technology (MIT) Media Lab Digital Currency Initiative (DCI)

---

1. The Digital Currency Initiative (DCI) is a group based at the MIT Media Lab focusing on digital currencies and their underlying technologies. One of the DCI's current projects is digital fiat currency (DFC) which is addressing how fiat currencies like the krona can be exchanged using blockchain technology without relying on existing banking infrastructure.

2. This document sets out our responses to the Riksbank's recent set of questions on developing a technical solution for a potential e-krona. We are currently working with a small group of central banks to research how a DFC could be implemented.

What would a technical solution for a register-based e-krona look like?

3. The most important consideration when developing a technical solution for transacting money is resilience – to both failure and deliberate attack. Different architectures achieve resilience in different ways, table 1 summarises these:

Table 1: Achieving resilience in centralised and decentralised systems

	Centralised	Decentralised
Resilience to failure	Backup system(s) which can take over if the main system fails.	A network of machines which can tolerate the failure of any individual element within the system and continue to function.
Resilience to attack	Increasing the cost of attack by creating a boundary which walls off the system and prevents unauthorised access.	Increasing the cost of attack by requiring an attacker to compromise a large number of nodes in order to make the system fail.

4. There is a distinction between a decentralised and a distributed system. It is possible for a single entity to deploy distributed systems to gain the resilience to failure outlined in table 1. In that instance, the resistance to attack could be achieved by creating a boundary around the whole distributed system. By contrast an open, decentralised system (such as Bitcoin) needs to be able to tolerate malicious nodes as anyone can join the system.

5. Also, centralisation of any given system is a spectrum rather than a binary choice. In reality a centralised system with multiple backups is a distributed system of sorts so the real question is the degree of centralisation rather than whether a system is centralised or not.

Cryptokernel

6. To further research the question of a technical solution for e-krona (or any other DFC) we would propose using Cryptokernel – the blockchain toolkit we have developed at MIT. Cryptokernel's basic architecture is similar to Bitcoin but the codebase is written from scratch

in C++. It uses the Lua scripting language for smart contracts. Cryptokernel takes the middle path between the Bitcoin scripting language (deliberately simplified, not Turing complete and cannot inspect blockchain state) and Ethereum (Turing complete and capable of creating new transactions automatically). Cryptokernel's approach is to have a Turing complete language but limited to inspecting the state of the blockchain and deciding whether a transaction was valid or not.

7. Cryptokernel is flexible enough to implement different configurations for different types of digital currency from a standard proof of work cryptocurrency (similar to Bitcoin) to a DFC. To test the Cryptokernel software we have used it to implement a coin called K320. The instructions for running a K320 node and the Cryptokernel source code are available on our website: http://dci.mit.edu/cryptokernel_k320.html.

8. The Cryptokernel software runs on Linux, MacOS and Windows platforms using commercially available hardware. As part of the research we are considering how Cryptokernel can be integrated with a central bank's RTGS system to allow a privately issued DFC to be fully backed by central bank money.

What challenges and opportunities do you envisage with each e-krona solution?

9. One challenge will be creating an e-krona which is resilient. If there is both a value based and register based e-krona another issue will be how the two forms of currency are exchanged.

10. For greatest resilience the value-based and register-based e-krona systems should be operationally independent of each other so failure in one does not affect the other. Users should be able to exchange one form of e-krona using entities which are capable of holding both forms of the currency. The mechanism could be similar to the function performed by ATMs, which are essentially machines for swapping one form of currency for another (physical cash and commercial bank deposits). As there is no physical element the mechanics would be different, especially in relation to distribution, but the concept would be similar.

11. Creating resilience means both addressing the architectural considerations set out above (such as the technology used and the degree of centralisation) and experimenting with possible solutions to see how they perform at scale and in a hostile environment. Penetration testing should be a key part of any system, ideally via a live deployment of a test system rather than an internal proof of concept with limited access.

12. A significant consideration will be where the e-krona should sit on the centralisation spectrum. More copies of the ledger increases resilience but at the cost of speed. Using a single central database would give a high throughput for transactions but presents a single point of failure which an attacker could exploit. The RIX system overcomes this problem by limiting access to a small set (fewer than 30)[1] of highly regulated institutions. As the e-krona is intended to have much broader availability (to the general public) it will also be exposed to a much larger pool of attackers than RIX so the architecture may need to be different to reflect this reality.

[1] http://www.riksbank.se/en/Financial-stability/The-RIX-payment-system/Participants/RIX-participants/

13. The main opportunities from releasing a register-based e-krona is the chance to shape standards for how DFCs should operate and to provide a platform for innovation. Taking these opportunities depends on the ecosystem surrounding the e-krona.

What is your vision for an e-krona, are there other possible solutions than register-based and value-based that you consider to be more appropriate?

14. Answering the solutions question depends on how the concept of a register-based e-krona system is interpreted. If the definition in the Riksbank paper[2] is applied narrowly – i.e. a central database – then there would need to be a third category which covered distributed systems. We have interpreted register-based e-krona to include distributed systems which means an additional category isn't needed.

15. Our vision for the e-krona is as part of a new decentralised financial system with greater resilience and closer to its users. Creating the e-krona (and other DFCs) in a way which can integrate with other parts of the system such as smart contracts and cross chain swaps will be important to its long-term usefulness.

What is missing in our concept?

16. The analysis in the paper takes the starting point as the existing financial system, it may also be worth approaching the question of issuing e-krona from the perspective of technology. This characterises the financial system as a stack of services from the simplest (payments) to the most complex (derivatives), each building on the other. Conceiving of the e-krona as a piece of technology as well as a payment system/currency would add a useful strand to the analysis. Taking the web/internet ecosystem as an example, this demonstrated that for global systems, open technology eventually wins out over proprietary technology:

Table 2: Open technology layers

Protocol/standard	**Platform**	**Created at**	**Body**
HTTP/HTML	Web	Cern	W3C
TCP/IP	Internet	Darpa	ICANN
Ethernet	Networking	Xerox Parc	IETF

17. As there are several different technologies promising to digitise national currencies the risk is choosing the wrong option and having to build another e-krona system a few years later. The way of minimising this risk is to run several e-krona experiments in parallel using different technology and challenge each one on how it interoperates with other technology. For example, one simple test could be to swap e-krona with a non-fiat cryptocurrency such as Bitcoin.

Robleh Ali
MIT Media Lab, Digital Currency Initiative
October 20, 2017

[2] http://www.riksbank.se/Documents/Rapporter/E-krona/2017/rapport_ekrona_170920_eng.pdf