SEAVUS INPUT TO THE DESIGN OF THE E-KRONA

Seavus group hereby present a short input concerning the project regarding implementing e-krona concept as an answer to the announcement on Riksbankens homepage.

As described in our cover letter, Seavus is widely experienced in the financial and monetary markets, latest technology areas and digitalisation of payments using cryptocurrencies and digital ledgers. Considering the short time we had for preparing this input, we are able to provide only conceptual proposal of the concept implementation at this moment.

We sincerely hope our input to e-krona project will help in generating good ideas and concepts and start of realization of the e-krona.

1. OVERALL ARCHITECTURE – A POTENTIAL PLATFORM

Overall solution can be a centralized consortium blockchain solution, which may be a hybrid solution of decentralized solution for the value-based usage and centralized solution for issuance and register based solutions. As candidates for this kind of currency, we propose a hybrid solution of Bitcoin[1] as a decentralized solution that provides anonymous or pseudonymous transactions as the value-based level of the system, and RSCoin[2] or a similar implementation like FedCoin[3] implementations for the permissioned minting (register) level above the value-based level. At the highest level, this architecture has one centralized authority that controls the work of the registers/mintees.

The proposed architecture is consisted from three layers:

1. **Controller layer** - where the national bank controls the register based market
2. **Register layer** - the controlled peer to peer distributed chain holding the ledger
3. **Consumer layer** - anonymous/pseudo-anonymous/pseudonymous peer to peer blockchain which represents the retail world.

1.1 CONTROLLER LAYER

The hybrid solution would have one centralized node, the national bank, which would dictate the exchange rates and the ties with the fiat unit. The central bank will operate with predetermined or on demand number of e-kronas (digital currency), creating a variable number of e-kornas as freshly mint value, rather than leaving this open to the winning miner. This would be the replication of the model for how central banks currently provide cash by issuing banknotes in order to meet customer requests, by redeeming central bank deposits.

The central bank prints cash on demand, and in this case the bank will have ability to issue digital currency e-kronas on demand. The central bank will have ability to redeem not needed e-kronas and issues banknotes in their place if needed. The National bank would then be responsible for issuing and reducing the number of e-kronas as well as changing their value in comparison with the fiat krona, if needed. Central bank may choose to have guarantee the one-to-one equivalence between digital e-krona and physical banknotes or have managed peg or let it float.

Seavus Stockholm AB – ingår i Seavus Group. Blekholmstorget 30, Hus F plan 10, 111 64 Stockholm

Info_SE@seavus.com • www.seavus.se

1.2 Register Layer

As proposed in the RSCoin the underlying system below controller layer, which will be audited and overseen by the central node, is consisted of decentralized known nodes. Each of these nodes will be a known node and will represent a register unit. The central bank can give licenses to these known nodes and define the case if these nodes are only banks, or other bodies (if we use the PSD2 terminology PISP's) can also be accepted in this group. Each node on this level will contain each record of the register and will participate in the consensus. If we go further in the PSD2, some of these nodes can become AISP, providers that have the complete list of registers and can access information, but do not have the permission to execute payment or join in the consensus process. These makes it easier for new players to both become PSD2 compatible and enter in the digital currency. Users may create accounts with these nodes (or have existing ones if this nodes are banks).

Each of these nodes as in RSCoin (under this proposal known as mintees), will be controlled by the central bank. The central bank is going to control the amount of e-currency produced in any of the entities. If the entities are doing the prove-of-work procedure to control and spread the resources, but take into account never to reach a monopoly and create possibility for the "51% Attack" when most of the cryptocurrency transactions will depend on a single financial entity that does the registration. We propose prove-of-steak instead of prove-of-work, due to the enormous energy and transaction time waste, when the ownership prove is done with the prove-of-work.

1.3 Consumer Layer

The lowest level in this "three tier" high-level architecture is the Consumer layer (actual users layer), where companies and people not involved in the register-based process can actually do decentralized transfers and register them with the known distributed ledgers. Each user can register a "digital wallet" (account) with any of the registers and gain access to the trade. The users, when doing transactions will execute a registration of ownership against this registers (mintees). The value-based currency in this case can be dispensed at ATM machines in exchange for fiat currency (Euro, SE Krona, or any other currency the providers see fitting), or topped with card payment (credit, debit). These e-currency cards, may be reusable and topped with fiat currency or by online banking, contact will be needed with one of the ATM's of the register that provides that card. These value-based e-krona will enable anonymous transactions like today cash.

Banks/Payment Providers that issue these cards may be interested in issuing contactless cards with expiration date, which can be also used and topped by online banking, ATM's or any other means. Digital wallets, can implement a known protocol, i.e. Bitcoin protocol to connect to the system. This is added value to the system so more apps from third party providers can be connected to the system, and opens the possibility to connect to existing payment service providers.

Users can connect their digital wallet with known bank channels or over PSD2 and have direct connection with the registers. Any app that does not have internet connection, and communicates with app that does not have internet connection shall send data immediately after it gets network connectivity. E-krona cards can also be associated with an existing fiat currency account. In this case, the exchange, if any, can be performed at the point of transaction.

Seavus Stockholm AB – ingår i Seavus Group. Blekholmstorget 30, Hus F plan 10, 111 64 Stockholm

Info_SE@seavus.com • www.seavus.se

2. Challenges

Challenge is education, market readiness, crimes and fraud that may rise with cashless system, and especially with centralized blockchain systems – that is why we propose banks as trusted party as register service providers.

Challenges during the implementation of the concept:

- How to link and relate existing payment systems and actors around the currency
- How to handle the large amount of payments
- How to handle offline payments
- AI as part of the monitoring and defence layers
  etc…

3. References

Please find the references below; the hybrid model assures that the best from all of the contenders is implemented, while eliminating the features that go against the requirements for the e-krona. Most of known blockchain security flaws are described in the references, also some specific to the proposed protocols.

[1] **Bitcoin**, https://bitcoin.org/en/, has been around since 2009 and it is the currently most valuable cryptocurrency

[2] **RSCoin**, http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf , is a project of the University College of London, and one of the candidates for Cryptocurrency at Bank of England

[3] **FedCoin**, https://law.yale.edu/system/files/area/center/global/document/411_final_paper_-_fedcoin.pdf, is a protocol and cryptocurrency that is currently a candidate for US Cryptocurrency

4. Contact

Dimitris Panagio, CEO Seavus Stokholm AB (former Ontrax AB)

dimitris.panagio@seavus.com