Central Banks around the world have been researching and implementing Central Bank Digital Currencies (CBDCs). One promising project in this field has been the MIT DCI’s openCBDC, which offers a very performant UTxO based cash-like retail CBDC payment processor system. It is a great candidate for expansion and testing with a digital identity framework that follows the SSI model.

Digital identity frameworks, specifically SSI have been identified in the literature as possibly playing an important role in CBDC design, although no specific design is in existence yet. The combination of SSI and CBDCs may allow for more complex financial workflows, better privacy, and simpler KYC processes, while mostly preserving performance.

We implemented a transaction workflow over openCBDC using Hyperledger Indy, which is a distributed ledger purpose built for digital identity management. Our goals are first to find out how does a simple SSI based identity management system interact with openCBDC, which is a non-DLT CBDC, and automate a simple KYC process. Second, introduce cash-like encumbrances taking advantage of openCBDC’s already cash-like design and SSI’s privacy capabilities.

These encumbrances include, as identified by the FSTRG research group at BTU, personal holding limits, and personal money flow limits. While a digital asset incorporating these encumbrances in addition to low-KYC prove to be closer to physical cash, the workflow enabling them may impact performance negatively.

Our approach is to use established cryptographic algorithms and protocols, over openCBDC and Hyperledger Indy to achieve these encumbrances, while acknowledging privacy and performance considerations.

In recent years, central banks around the world have been researching the possible introduction of Central Bank Digital Currencies (CBDCs); digital currencies which are directly backed by the central bank. A wide range of CBDC models and hosting architectures have been explored, from classic bank account like money to Bitcoin-style bearer instruments, and from centralized solutions to compositions of decentralized systems. However, despite the large number of publicized experiments, open prototypes are extremely scarce and key questions of identity handling and privacy are mostly left open with a simple reference of these being dependent on central bank policy decisions.

At the same time, digital identity handling is undergoing its own revolution. With markedly different emphases, “flavors” and relationships, but initiatives as Self-Sovereign Identities (SSI) and Decentralized Identities share the common idea that the many identities of a person should be tied to personal “wallets” and credentials should be issued against these. Decentralized ledgers form an important part in securing these approaches. However, it has been only recognized that SSI should bform an important component in CBDC security, auditability and privacy – as of now, analyses on the specific possible approaches are practically nonexistent.

In this work, my first contribution is mapping out and prototyping the payment identity support capabilities that the leading SSI technology stack, Hyperledger Aries and Indy can bring to the practically only open source CBDC payment processor solution, openCBDC from the Digital Currency Initiative of MIT. Importantly, the use cases include Know-Your-Customer requirement support and authentication and authorization for payment.

Second, while CBDCs will not generally be cash-like in their privacy – as they are digital assets – the need of the public for the level of privacy provided by cash will have to be recognized. I propose that a special CBDC asset in a full CBDC ecosystem, which has artificial cash-like encumbrances – as maximum holdable amount, low speed of money and physical closeness of payer and payee – could be allowed to function with cash-like privacy. To this end, drawing on the presence of an SSI stack, I propose and prototype a payment protocol for openCBDC, inspired by Chaumian DigiCash, which on the one hand enables users to utilize any number of Bitcoin-like pseudonyms with the default level of privacy in Bitcoin, and on the other hand, ensures the presence of these (parameterizable) “encumbrances”, which mimick the physical properties of cash.

1. Információs rendszerek
2. Szoftver