Payments in openCBDC with Self-Sovereign Identitites – from the verifiable to the private

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 only been recognized that SSI should form 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 proximity 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 mimic the physical properties of cash.

Fizetések nyílt CBDC-ben ön-szuverén azonosítókkal – az ellenőrizhetőtől a privátig

Az elmúlt években a világ központi bankjai a Digitális Jegybak Pénzek (CBDC) lehetséges bevezetését kutatták; digitális valutákét, amelyeket közvetlenül a központi bank fedez. A CBDC modellek és kiszolgálási architektúrák széles skáláját vizsgálták meg, a klasszikus bankszámla jellegű digitális pénztől a Bitcoin-stílusú pénzügyi eszközökig, valamint a központosított megoldásoktól a decentralizált rendszerekig. A nyilvánosságra hozott kísérletek nagy száma ellenére azonban a nyílt forráskódú prototípusok rendkívül ritkák, valamint az identitáskezelés és a titoktartás kulcskérdései többnyire nyitva maradnak, egyszerű hivatkozással arra, hogy ezek a jegybank politikai döntéseitől függenek.

Ugyanakkor a digitális személyazonosság-kezelés saját forradalmán megy keresztül. Az olyan kezdeményezések, mint a Self-Sovereign Identities (SSI) és a Decentralized Identities azt a közös elképzelést vallják, hogy egy személy sokféle identitását valamilyen személyes „pénztárcához” kell kötni, és erre kell hitelesítő okiratokat kiadni. Az elosztott főkönyvek fontos szerepet játszanak ezen megközelítésekben. Azt azonban csak nemrég ismerték fel, hogy az SSI-nak a CBDC biztonságának, auditálhatóságának és adatvédelmének fontos elemét kell képeznie – a konkrét lehetséges megközelítésekre vonatkozó elemzések egyelőre gyakorlatilag nem léteznek.

Ebben a munkámban az első hozzájárulásom azoknak a fizetési identitás-támogató képességeknek a feltérképezése és prototípusának elkészítése, amelyeket a vezető SSI technológiai halmaz, a Hyperledger Aries és az Indy hozhat a gyakorlatilag egyetlen nyílt forráskódú CBDC fizetési rendszerhez, az MIT Digital Currency Initiative-jából származó openCBDC-hez. Az implementált funkciók közé tartozik az „Ismerd meg ügyfeled” követelmények támogatása, valamint a hitelesítés és a fizetésre való authorizáció.

A második pedig, hogy bár a CBDC-k titoktartást tekintve általában nem készpénzszerűek – mivel digitális eszközökről van szó –, el kell ismerni a közvélemény igényét a készpénz által biztosított titoktartás szintjére. Javaslom, hogy egy speciális CBDC eszköz egy teljes CBDC ökoszisztémában, amely mesterséges készpénzszerű „terhekkel” rendelkezik – mint például a maximálisan tartható összeg, a pénz alacsony sebessége, valamint a fizető és a kedvezményezett fizikai közelsége – elősegíthetné a készpénzszerű titoktartást. Ebből a célból, egy SSI protokol rendszerre támaszkodva, egy fizetési protokollt és egy prototípust készítek az openCBD-hez, amelyet a Chaum-i DigiCash ihletett, amely egyrészt lehetővé teszi a felhasználók számára, hogy tetszőleges számú Bitcoin-szerű pszeudonímát használjanak a Bitcoinban ismert adatvédelmi szint mellett., másrészt biztosítja ezen (paraméterezhető) „terhek” működését, amelyek a készpénz fizikai tulajdonságait hivatottak emulálni.