DIGITÁLIS JEGYBANKPÉNZEK

Kriptovaluta helyett elektronikus készpénzt!


GÖNCZY LÁSZLÓ, BME VIK

FORRÁS: BME VIK


KOCSIS IMRE, BME VIK

FORRÁS: BME


SZOMBATI ANIKÓ, MNB

FORRÁS: MNB

Az alternatív pénzügyi szolgáltatók és a kriptopénzek feltűnése és népszerűvé válása nemcsak a kereskedelmi bankokat állította nehéz helyzet elé, hanem a jegybankokat is lépéskényszerbe hozta. Válaszul ők is vizsgálják saját digitális pénz bevezetését.

Alanyi jogon járó, ingyenes elektronikus bankszámla, a készpénzhez hasonlóan bárhol könnyen használható digitális pénz, a számlákhoz kapcsolódó innovatív szolgáltatások – mindezt, sőt ennél is többet ígérnek az úgynevezett digitális jegybankpénzek (DJBP, avagy közkeletű angol elnevezéssel CBDC, central bank digital currency).

De miért is foglalkozik a DJBP-vel gyakorlatilag a világ összes jegybankja? A digitális jegybankpénzt voltaképpen a kényszer szülte (vagy inkább még szüli). A digitalizálódás, és különösen

a kriptopénzek megjelenése olyan kihívások elé állította a jegybankokat, amelyekkel korábban nem találkoztak – például hogyan tartsák fenn a pénzügyi szuverenitást, ha az ország polgárai, vállalkozásai valamilyen globális vállalat által kibocsátott pénzügyi eszközben fizetnek?

Mindenkinek jár

A jegybankok manapság kétféle pénzt bocsátanak ki. Az egyik a készpénz, a másik a számlapénz, utóbbi azonban csak a kereskedelmi bankok és bizonyos állami intézmények számára elérhetők, csak ezek vezethetnek számlát a jegybanknál. Ha az állampolgárok vagy a vállalkozások számlát szeretnének nyitni, a kereskedelmi bankokhoz kell fordulniuk. A bankoknál tárolt pénz viszont ki van téve némi kockázatnak, hiszen a bank bedőlésével elveszhet a pénz egy része is.

Digitális jegybankpénzzel megoldható, hogy a szervezetek egymás között okos szerződések alapján automatikusan végbemenő tranzakciókat bonyolítsanak le

„A digitális jegybankpénzzel új fizetési forma jelenhetne meg”, mondta a BME VIK rendezésében nemrégiben megtartott online konferencián *Szombati Anikó,* a Magyar Nemzeti Bank digitalizációért és fintech-fejlesztésért felelős ügyvezető igazgatója. Elvileg nincs akadálya, hogy minden magánszemélynek és minden vállalkozásnak, szervezetnek legyen DJBP-számlája, vagy hozzáférjen azzal egyenértékű (akár ingyenesen kínált) szolgáltatáshoz. Döntéstől függően létrehozható olyan DJBP, amely digitális készpénzként viselkedik: alanyi jogon hozzáférhető fizetőeszköz, korlátlanul és kockázat nélkül lehet vele egymás között tranzakciókat lebonyolítani vagy fizetni, ráadásul innovatív szolgáltatások építhetők rá.
A BME és az MNB átfogó együttműködésének keretében, a Villamosmérnöki és Informatikai Kar (VIK) a digitális jegybankpénz blokklánc és elosztott főkönyv (DLT, distributed ledger technology) alapú technológiai megvalósíthatóságán dolgozik. „Azt vizsgáljuk, hogy milyen technológiák alkalmasak erre, miként lehet megfelelni a megbízhatósági és teljesítménykövetelményeknek. Emellett azon is gondolkodunk, hogy a kialakítandó DJBP rendszer miként tudja támogatni az okos szerződéseken alapuló innovációt”, mondja *Kocsis Imre,* a BME VIK Méréstechnika és Információs Rendszerek Tanszékének adjunktusa. Az ipari alkalmazások kutatása a Távközlési és Médiainformatikai Tanszékkel szoros kooperációban, *Varga Pál* tanszékvezető docens vezetésével folyik.

Automatikus tranzakciók

Az egyetem szakemberei már össze is állítottak egy prototípust a lehetőségek feltérképezésére – hangsúlyozva, hogy ez még nem az MNB elképzelései szerint történt, a tervezés ugyanis még messze nem ért ebbe a fázisba. Létrehoztak egy, a nyílt forráskódú Hyperledger Fabric-on alapuló DJBP-blokkláncot és mellé egy, az alkalmazásokat támogató Ethereum-hálózatot, és azt tanulmányozzák, miként lehet az egyikből a másikba átvinni a DJBP-t megszemélyesítő tokeneket, és azokat milyen alkalmazási esetekre lehet használni.
Az egyik ilyen eset lehet a vállalatközi blokklánc-hálózatok szereplői közötti elszámolás. Jelenleg ugyanis hiába számolnak el egymással a vállalati szereplők a blokkláncon belül bármilyen coin-ban, tokenben, kell egy vagy több olyan fél, amelyik valós pénzbeli fedezetet is nyújt ezekre az elszámolóegységekre, illetve amelyek egymás között, a jegybank közbeiktatásával, a pénzbeli elszámolásokat is elvégzik, mondja Kocsis Imre. Vagyis ahhoz, hogy az elszámolás tényleg valós időben és valós pénzben megtörténjen, szükség van pénzintézet részvételére vagy egy tradicionális, külső „elszámolási lábra”.
A DJBP megoldást kínál erre a problémára, mert a digitális jegybankpénzt be lehet vonni a vállalatközi vagy egyéb együttműködésekbe. A DJBP-vel megoldható, hogy a szervezetek egymás között okos szerződések alapján automatikusan végbemenő tranzakciókat bonyolítsanak le, mégpedig olyan eszközben, amely nem volatilis, és megbízható szereplő biztosítja a stabilitását.
Ezek után nincs szükség egyetlen központi szereplőre az elszámolásokhoz, mert a blokklánc megteremti és garantálja a résztvevők közötti bizalmat. Mindennek köszönhetően sokkal gyorsabbá, hatékonyabbá és transzparensebbé válhatnak az egymás között zajló folyamatok és nagy mértékben automatizálhatók a tranzakciók.

Nem teljesen anonim

Ugyanakkor még számos szabályozási és technológiai kérdést kell tisztázni addig, amíg a DJBP-ből valóság lesz. Ilyen például a biztonság kérdése, említett egy példát *Gönczy László,* a Méréstechnika és Információs Rendszerek Tanszék adjunktusa. Nem csak arra kell figyelni, hogy a kommunikáció során ne sérüljön az adatok integritása, de azt is előzetesen bizonyítani kell, hogy az okosszerződések nem játszhatóak ki – nem fordulhat elő például, hogy megérkezik az áru, de nem utalódik át a pénz. Természetesen az is kulcsfontosságú, hogy a DJBP-t ne lehessen kilopni a digitális tárcákból, mint ahogy az már több kriptovalutával megtörtént.
A szabályozás során eldöntendő kérdés, hogy mennyire legyen anonim a digitális jegybankpénz. A BME kutatói egy pszeudonimizáló, félig anonim rendszert alkottak meg, az Ethereum privát-publikus kulcspár megközelítésére alapozva. Ebben a felhasználó a privát kulcsával indítja a tranzakciókat, de nem a főkönyv (ebben az esetben a jegybank) tartja nyilván, hogy ki áll a kulcs mögött. Erre a célra a szakemberek egy közbülső szintet építettek a rendszerbe (ezek lehetnének majd a kereskedelmi bankok), amelyek nyilvántarthatják, hogy ki áll a kulcspár mögött. Így bizonyos mértékig visszakövethetővé válna a DJBP, amire valószínűleg szükség is lenne, hiszen hibás teljesítés vagy reklamáció esetén a kiinduló állapotot vissza kell állítani. Azt is meg kell oldani, hogy miként juthat a digitális pénzéhez a felhasználó, ha a kriptográfiai kulcsokat tároló eszközét (mobiltelefonját, kártyáját) elvesztette, ellopták.

Schopp Attila

A kvantum sem jelent veszélyt

Sokszor hallani, hogy a gyakorlati alkalmazáshoz egyre közelebb álló kvantumszámítógépeknek nem okoz majd nehézséget a jelenleg alkalmazott – és a DJBP-hez is használt – digitális aláírások feltörése. Mégsem kell félni attól, hogy a kialakítandó DJBP-infrastruktúrák hirtelen sérülékennyé válnának, nyugtat meg mindenki Kocsis Imre. Már jelenleg is léteznek „kvantumrezisztens” aszimmetrikus digitális aláírási és titkosítási algoritmusok, amelyek a jelenlegi ismeretek szerint kvantumszámítógéppel sem törhetők fel.