A blokklánc technológia a pénzmosással szemben

Kenéz Dávid

DOI: 10.14267/VILPOL2023.04.07

A 21. század egyik legfontosabb találmányaként tartjuk számon a blokkláncrendszereket és a kriptovalutákat. Ezeknek a rendszereknek számtalan felhasználási lehetősége van, képesek a tulajdonosi lánc és az eredetiség igazolására, forradalmasíthatják a kereskedelmet az ún. okos szerződések segítségével, sőt egyes vélemény szerint akár teljesen megváltoztathatják a jelenleg ismert bankrendszer szükségességét. Ugyanakkor fontos tudnunk, hogy a blokkláncok legalább annyi veszélyt hordoznak, mint amennyi problémára megoldást kínálnak. Ezen kockázatok közé tartozik a terrorizmus finanszírozásának és a pénzmosásnak a veszélye is.

A terrorizmus finanszírozásának két hagyományos módja van: az ún. Hawala hálózat, valamint a nemzetközi bankrendszer. A Hawala hálózat, azaz az informális átutalási rendszer a több forrásból származó ügyletei következtében nehezen követhető le, ugyanakkor a bizalmi problémák és a számos forrása miatt túl lassú és nem elég dinamikus a hatékony finanszírozásra. Másik a hagyományos bankrendszer, ami egyfelől centrális és gyors, mindazonáltal az egyre fejlődő AML/CTF rendelkezések[1] megfelelése miatt manapság már egyre könnyebben szűrhető.

Ezeket a problémákat küszöbölik ki a blokkláncok a terroristaszervezetek számára, azáltal, hogy lehetővé teszi számukra, hogy megbízzanak egy harmadik személyben, anélkül, hogy ehhez egy közvetítőt kellene igénybe venniük. A blokkláncokat és a hozzájuk kapcsolódó kriptovalutákat eredetileg éppen azzal a céllal hozták létre, hogy ezáltal „kikerülhetők" legyenek ezek a közvetítő intézmények, és ezáltal egy gyorsabb, olcsóbb és biztonságosabb módszert hozzanak létre a pénzügyi tranzakciók lebonyolítására. Ugyanakkor éppen ezek a közvetítő intézmények töltik be az „őrök" szerepét a pénzmosás és a terrorizmus finanszírozása elleni harcban. A bűnelkövetők a kripto-valuta keverő szolgáltatások, illetve a Dark Wallet nevű program segítségével tudják lekövethetetlenné tenni a tranzakcióikat, ezáltal megőrizve az anonimitásukat a jogszabályok megkerülésével.

Jó hír azonban, hogy a blokkláncok és kriptovaluták jelentette veszély kezelhető. A blokkláncok előnye, hogy az állami hatóságok számára követhetővé teszik minden jelenlegi és korábbi kriptovaluta tulajdonosának forgalmát, amennyiben lehetővé tesszük az államok számára a blokklánc elérését. Azonban ennek megvalósítása során két problémával is szembesülünk. Az első probléma az, hogy a tranzakciók érvényesítéséhez a blokkláncot működtető számítógépek, az ún. „node-ok" legalább felének a „jó fiúk" kezében kell lenniük. A második probléma az, hogy jelenleg a tranzakciók névtelenül zajlanak, vagyis nem ismerjük azt a személyt, aki az ellopott kriptovalutát birtokolja, ez pedig megnehezíti az igények érvényesítését.

Az első problémára az jelentheti a megoldást, ha létrehozunk egy állami blokkláncot, amelynek valamennyi node-ja az állam tulajdonában áll. Ebben az esetben biztosak lehetünk, hogy csak olyan

[1] AML/CTF rendelkezések: a pénzmosás és a terrorizmus finanszírozása elleni küzdelemre vonatkozó szabályok

tranzakciókat hitelesít a rendszer, amelyek legálisak. Akár kialakítható lehetne egy EU blokklánc is, ráadásul, ha lehetővé tesszük, hogy egy ilyen blokklánchoz valamennyi tagállam hatóságai hozzáférhessenek, akkor az megkönnyítené a tagállamok nyomozóhatóságai közti együttműködést is. A második probléma megoldását jelentené egy olyan reguláció, miszerint a digitális pénztárcákra úgy kell tekinteni, mintha bankszámlák lennének, a digitálisvaluta-váltókra pedig úgy, mintha „rendes" pénzváltó helyek lennének. Mindez több jogkövetkezménnyel is járna, révén ennek megfelelően vonatkoznának az ilyen rendszerek üzemeltetőire a pénzügyi szolgáltatásokkal kapcsolatos jogszabályok. Emellett a terrorizmus finanszírozása a veszélyének további csökkentése érdekében a pénzügyi szolgáltatókra vonatkozó AML/CFT szabályokat is szigorítanunk kellene.

Tehát a blokkláncok valóban megoldást jelenthetnek a kriptovaluták által okozott veszélyekre, így kihasználhatjuk a bennük rejlő potenciált a pénzmosás és más bűncselekmények felderítésére. A blokkláncokban minden tranzakciót rögzítenek, amelyek nyilvánosan elérhetőek, és bár az ember számára a kriptovaluta útja nyomon követhetetlen lehet, egy pénzmosáskockázat-elemző program futtatásával az illegális tevékenységekből származó összegek azonosíthatóvá válhatnak. Az ügyfél-megismerési szabályok kötelezővé tétele a blokkláncokkal kapcsolatban lehetővé teszi az érintett digitális pénztárcák tulajdonosainak azonosítását.

Fontos ugyanakkor megjegyezni, hogy a blokkláncokkal kapcsolatos átláthatóság és az anonimitás elvesztése egyesek számára ellentmondásos lehet, és akár eltántoríthatja a befektetőket, valamint visszavetheti az innovációt. Az anonimitás ugyanakkor eleve nem teljes a kriptovalutáknál, mivel a tranzakciók nyilvánosak. Azonban az illegális szolgáltatások használhatnak olyan eszközöket, amelyek segítségével még inkább növelhetik az anonimitást, így további kihívásokat jelenthetnek a hatóságok számára. Ezen eszközök használata természetesen magas szintű számítógépes ismereteket igényel, ezért egyes terroristaszervezetek a közösségi médiát veszik használatba, hogy megosszák egymás között a módszereiket. Amíg ezeket a lehetőségeket nem zárjuk el a bűnözők elől, addig hiába vezetjük be a „know-your-customer" szabályokat a digitális pénztárcák és kriptovalutaváltók területén, a terroristák mindig egy lépéssel a hatóságok előtt tudnak járni.

A másik megoldatlan probléma az, hogy különböző államok eltérően minősítik az egyes magatartásokat bűncselekménynek. Mivel a blokkláncok határokon átnyúló tranzakciókra is alkalmazhatók, ez okozhat kihívásokat a joghatóság és jogi normák terén. Az államoknak felmerülő bűncselekmények esetében egyeztetett protokollokat kell kidolgozniuk, valamint gondoskodniuk kell a megfelelő programokról az illegális tevékenységek monitorozására. A transzparencia és a magánérdekek összehangolása szintén komplex kérdés. A felhasználók jogi védelme fontos, különösen az üzleti titok tekintetében, hogy vállalkozások adatai ne legyenek illetéktelenek számára hozzáférhetők. A blokkláncok tehát valóban sok lehetőséget rejtenek, de egyúttal számos kihívást is felvetnek, és a megoldások kidolgozása szerteágazó együttműködést igényel nemzetközi szinten is.