Gond van a Bitcoin jövőjének szánt technológiával

**A SZTAKI kutatói - Béres Ferenc és Benczúr András, valamint az ELTE doktorandusza, Seres István - hálózattudományi eszközökkel is megvizsgálták a Bitcoin problémáinak – lassúság, nehezen skálázhatóság – megoldására szánt, jelenleg legnépszerűbb, úgynevezett fizetési csatornáját, a** [**Lightning Network**](https://lightning.network/)**öt. A végeredmény: a megoldás nem eléggé anonim, és egyáltalán nem biztos, hogy működni fog.**

 A Bitcoin, az Ethereum és más kriptopénzek új típusú, ún. bizalmat nem feltételező digitális fizetőeszközök, amelyek nagy előrelépést jelentenek a szükséges bizalom minimalizálásában: kriptopénzekkel anélkül lehet pénzt küldeni bárhova a világon, hogy ehhez meg kellene bíznunk bármilyen bankban vagy más pénzügyi közvetítőben. Ráadásul a rendszer teljes állapotát - beleértve az összes tranzakciót – eltárolják a blokkláncban, így az nyilvánosan ellenőrizhető.

A decentralizációnak és a nyilvános ellenőrizhetőségnek viszont ára van: a rossz skálázhatóság. A Bitcoin átlagosan másodpercenként 7 tranzakció feldolgozására képes, míg a legelterjedtebb, centralizált fizetési szolgáltatók (pl. Visa, Mastercard) csúcsidőben másodpercenként 40-50 ezer tranzakció feldolgozására képesek. Ráadásul, a kriptopénzes tranzakcióknál nem garantálható, hogy az elindításuk után azonnal teljesülnek, a tranzakciós díjak pedig nagyon volatirisek. A kriptopénzekkel foglalkozó közösség ezért folyamatosan megoldásokat keres a fenti problémák megoldására.

**Fizetési csatornákkal a blokklánc skálázhatóságáért**

Az egyik elterjedt skálázhatósági megoldás az úgynevezett fizetési csatorna hálózatok (payment channel networks) kiépítése: ezek plusz réteget képeznek a blokklánc felett. A fizetési csatornákon a felhasználók azonnal teljesülő kifizetéseket indíthatnak, és a legtöbb esetben a tranzakciós díjak is elhanyagolhatók.

A fizetési csatorna hálózatok megjelenése miatt a hálózattudomány is fontos szerephez jut a kriptogazdasági kutatásokban - ezen a ponton szálltak be a SZTAKI kutatói is: hálózattudományt használnak a Bitcoin fizetési csatornák kapcsolatainak feltérképezésére, és a rendszer gazdaságtanának jobb megértéséhez.

A fizetési csatornák rendszerét modellezhetjük irányított, súlyozott gráfokként, ahol a csomópontok a felhasználókat, míg az őket összekötő élek a fizetési csatornákat jelölik. Adott él súlya a fizetési csatornán lekötött kriptopénz mennyisége, azaz a kapacitás. Minden csatorna csak a saját kapacitását nem meghaladó összegű tranzakciók továbbítására képes. A felhasználók - a csatornakapacitásokat figyelembe véve - küldhetnek egymásnak kifizetéseket, amelyeknek érvényességét a csatornákon lévő fedezet garantálja. Ezzel, még ha nincs is közvetlen fizetési csatorna két résztvevő között, egy több csatornából álló út kijelölésével irányíthatnak kifizetéseket egymáshoz, akár nem megbízható feleken keresztül is. A kifizetéseket közvetítő csomópontok (router nodes) tranzakciós díjat szedhetnek a kriptopénz összegek továbbításáért, ezzel motiválva őket az általuk nyújtott szolgáltatásért.

**Mi a Lightning Network?**

A Lightning Network a Bitcoin egyik fizetési csatorna hálózata. Jelenleg ez a  legnépszerűbb és legelterjedtebb fizetési csatornákra épülő rendszer: több ezer felhasználója és több tízezer csatornája van. Sokak szerint a Lightning Network megoldja a Bitcoin skálázhatósági és anonimizálási gondjait, mivel a használatával a legtöbb kifizetést nem tárolják el a nyilvános, lassú és költségesen karbantartható blokkláncban, csak a felette lévő rétegben.

A SZTAKI kutatóit az érdekelte, mennyire teljesülnek valójában ezek az ambiciózus ígéretek. Az első és legfontosabb kérdés, hogy a központi router csúcsok elég motiváltak-e a kifizetések továbbítására. SZTAKI kutatói megfigyelték, hogy a Lightning Network központosított gráf, ahol a kifizetések túlnyomó részének továbbításáért csak néhány csomópont felelős. Ha ezek a csomópontok nem működnek, az egész hálózat működésképtelenné válik.

SZTAKI kutatói megállapították, hogy a jelenlegi használati szint és tranzakciós díjak mellett a központi  csomópontok lényegében nincsenek megfelelően ösztönözve a kifizetések továbbítására. Ha feltételezzük, hogy a fő közvetítő csomópontok pénzügyileg racionálisan viselkednek, nagyságrendekkel magasabb tranzakciós díjakra vagy forgalomra lenne szükség. Eredményeik alapján a Lightning Network – és néhány más, kisebb fizetési csatorna hálózat – valószínűleg csak néhány lelkes csomópont jóakarata miatt működik.

**Nem eléggé anonim**

Minden monetáris rendszernél alapvető feltétel, hogy védje felhasználói pénzügyi adatait. Az egyének és cégek érdeke, hogy titokban tartsák egyenlegüket és teljes tranzakciós történetüket. Egyelőre minden, adott Bitcoin-címhez tartozó tranzakció nyilvános, ezért, ha a Bitcoin-címet sikerül személyhez kapcsolni, automatikusan kiderül, mennyi van a számláján és milyen tranzakciói voltak.

A Lightning Network anonimizálási megoldása az úgynevezett onion routing: egy közvetítő nem ismeri a fizetési útvonalban betöltött helyét. Például, ha Alice kifizetését egy router csomópont továbbította Bobnak, akkor a router nem tudhatja, hogy azt Alice, Alice valamelyik szomszédja vagy azok szomszédai kezdeményezték.

Sajnos az onion routing nem elegendő az anonimizáláshoz. A SZTAKI kutatói a hálózat topológiájának vizsgálatával kiderítették: csak gyakori tévhit, hogy a fizetési csatornák erős védelmet biztosítanak a felhasználóiknak.

Mivel a Lightning Network - a közösségi hálózatokhoz hasonlóan - kis átmérővel rendelkezik (ún. [kisvilág-tulajdonságú](https://hu.wikipedia.org/wiki/Kisvil%C3%A1g-tulajdons%C3%A1g)), a legrövidebb és legolcsóbb út két résztvevő között gyakran csak két vagy három lépésből áll. A SZTAKI kutatóinak mérései szerint a router csomópontoknak erős statisztikai bizonyítékuk van egy kifizetés feladójáról és címzettjéről is a rajtuk átfolyó kifizetések több mint 50 százalékában – ami rontja a Lightning Network adatvédelmét és csökkenti a blokklánc helyettesíthetőségét. A SZTAKI kutatói arra számítanak, hogy eredményeik hatására még több hálózattudományi munka jelenik meg a kriptopénzek területén. Nagyon fontos megérteni és alaposan elemezni a kriptográfiai rendszereket hálózati szempontból is, mivel a kriptopénzek számos tulajdonsága (skálázhatóság, adatvédelem, résztvevők motiválhatósága) a tranzakciós hálózat topológiai tulajdonságaival áll kapcsolatban.

÷

*Az eredményeket a kutatók 2019. november 21-én, nyomtatás előtt közzétették, elérhető az arXiv:1911.09432,* [*https://arxiv.org/pdf/1911.09432*](https://arxiv.org/pdf/1911.09432) *címen.*

*Kutatásukra gyorsan felfigyelt a kripto-gazdasági közösség, kommentelte Twitteren Emin Gün Sirer, a Cornell kutatója, írtak róla angol, német és kínai szaklapok is.*

**További információk:**

**Sajtókapcsolat:**

Laza Bálint
laza.balint@sztaki.hu
+36 70 577 65 65

**Technikai kontakt:**
Benczúr András
benczur.andras@sztaki.hu

**Hasznos linkek:**

[A Lightning Network hivatalos oldala](https://lightning.network/)

[Bővebben a Lightning Networkről](https://en.wikipedia.org/wiki/Lightning_Network)

[A kisvilág-tulajdonság](https://en.wikipedia.org/wiki/Small-world_network)

**A SZTAKI-ról**

A Számítástechnikai és Automatizálási Kutatóintézet (SZTAKI) az ország legnagyobb és legsikeresebb informatikai kutatóintézete. A SZTAKI a tágan értelmezett informatika tudományának műhelye, az információtechnológia, számítástudomány és rokon területeinek nemzeti kutatóbázisa. Elsősorban az informatika műszaki-tudományos és matematikai kérdéseivel foglalkozik, de a kutatások kiterjednek mindazon területekre, amelyek az alapkérdésekkel kapcsolatban állnak. Az alap- és alkalmazott kutatás széles körű művelése mellett fontos feladat a megszerzett speciális ismeretek hasznosítása a kutatás-fejlesztés, rendszertervezés és rendszerintegrálás, tanácsadás, szoftverfejlesztés területén. A SZTAKI-ról [itt olvashat bővebben](https://sztaki.us4.list-manage.com/track/click?u=51b3fe8450ebdc0db77ec09e1&id=ab3ddcd21c&e=6a0917774a)