Kriptovaluták elméleti háttere

Ladóczki Bence
docens
Távközlési és Mesterséges Intelligencia Tanszék (TMIT)
Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar (VIK)
ladoczki.bence@vik.bme.hu

2026. november 3.

1 Monero: összegek, bányászat és használat

1.1 RingCT (Ring Confidential Transactions)

2017 óta a Monero a RingCT [1] protokollt alkalmazza, amely Pedersen-commitmentekkel (commitments) rejti el a tranzakciók összegét. A hálózat ellenőrizni tudja, hogy a bemenetek összege megegyezik a kimenetek összegével (nincs pénzteremtés), anélkül hogy bárki megtudná a konkrét összegeket. A Pedersen-commitment: $C = aG + bH$, ahol a az összeg, b a blinding faktor, G és H generátor pontok.

1.2 Range proofs: negatív összegek megakadályozása

A Pedersen-commitment önmagában nem elegendő: a csoportművelet additív, tehát a hálózat ellenőrizni tudja, hogy $\sum C_{\text{bemenet}} - \sum C_{\text{kimenet}} = 0$ (azaz a blinding faktorok is kiegyenlítődnek), de ez nem akadályozza meg a negatív összegek használatát. Például ha valaki -5 XMR-t és $+15$ XMR-t ad kimenetként egy 10 XMR bemenethez, az egyenleg stimmel ($10 = 15 + (-5)$), de a -5-ös kimenet a modulo aritmetika miatt egy hatalmas pozitív számként jelenne meg – így pénzt gyártottak volna a semmiből.

A megoldás a range proof (tartomány-bizonyíték): a küldőnek minden kimenethez bizonyítania kell, hogy az összeg egy érvényes tartományba esik, azaz $0 \leq a < 2^{64}$, anélkül hogy felfedné a pontos értékét. A Monero jelenleg Bulletproofs+ [2] mechanizmust alkalmaz erre:

- Az összeg bináris felbontását használja: $a = \sum_{j=0}^{63} a_j \cdot 2^j$, ahol minden $a_j \in \{0, 1\}$.
- Minden bithez egy Pedersen-commitmentt készít, és egy zero-knowledge bizonyítással igazolja, hogy az commitment valóban 0-t vagy 1-et tartalmaz.
- A Bulletproofs az egész bizonyítást logaritmikus méretűre tömöríti: 64 bit helyett $\approx 2\log_2(64) = 12$ csoportelem elegendő.

Így a hálózat meg tud győződni arról, hogy minden kimenet nem-negatív és legfeljebb $2^{64} - 1$, anélkül hogy megtudná a konkrét összegeket. Ez zárja ki a negatív összegekkel való pénzgyártást.

1.2.1 A Bulletproofs protokoll részletei

A Bulletproofs [2] egy interaktív bizonyítási protokoll (amelyet Fiat–Shamir heurisztikával nem-interaktívvá alakítanak). Két szereplője van: a bizonyító (prover, P) – aki a tranzakciót létrehozza és ismeri a titkos v összeget –, és az ellenőrző (verifier, V) – a hálózat bármely csomópontja, aki ellenőrzi a tranzakciót. A cél: P meggyőzi V-t, hogy a $V = h^{\gamma} g^{v}$ commitmentben lévő v a $[0, 2^n - 1]$ tartományba esik, anélkül hogy v-t felfedné.

A protokoll lépései:

1. lépés (P $\rightarrow$ V): Commitment-ek küldése.

P felírja v bináris kifejtését: $\mathbf{a}_L \in \{0,1\}^n$, ahol $\langle \mathbf{a}_L, \mathbf{2}^n \rangle = v$, és $\mathbf{a}_R = \mathbf{a}_L - \mathbf{1}^n$. A bit-feltétel ($a_{L,j} \in \{0,1\}$) ekvivalens azzal, hogy $\mathbf{a}_L \circ \mathbf{a}_R = \mathbf{0}^n$ (mert $0 \cdot (-1) = 0$ és $1 \cdot 0 = 0$). P választ véletlen α, ρ blinding faktorokat és $\mathbf{s}_L, \mathbf{s}_R$ véletlen vektorokat, majd elküldi V-nek:

$$A = h^{\alpha} \cdot \mathbf{g}^{\mathbf{a}_L} \cdot \mathbf{h}^{\mathbf{a}_R}, \qquad S = h^{\rho} \cdot \mathbf{g}^{\mathbf{s}_L} \cdot \mathbf{h}^{\mathbf{s}_R} \tag{1}$$

A a bit-vektor commitment-je, S a blinding vektorok commitment-je. V nem tudja kiolvasni belőlük $\mathbf{a}_L$-t vagy $\mathbf{s}_L$-t.

2. lépés (V $\rightarrow$ P): Challenge küldése.

V véletlenszerűen választ $y, z \in \mathbb{Z}_p$ challenge értékeket és elküldi P-nek. Ezek arra szolgálnak, hogy a három külön feltételt (összeg, bit-jelleg, $\mathbf{a}_R$ definíció) egyetlen belső szorzatra redukálják:

$$\left\langle \mathbf{a}_L - z \cdot \mathbf{1}^n,\ \mathbf{y}^n \circ (\mathbf{a}_R + z \cdot \mathbf{1}^n) + z^2 \cdot \mathbf{2}^n \right\rangle = z^2 \cdot v + \delta(y, z) \tag{2}$$

ahol $\delta(y,z) = (z - z^2)\langle \mathbf{1}^n, \mathbf{y}^n \rangle - z^3 \langle \mathbf{1}^n, \mathbf{2}^n \rangle$ egy V által önállóan kiszámítható korrekciós tag.

3. lépés (P $\rightarrow$ V): Polinom commitment-ek küldése.

P definiálja a vektorpolinomokat:

$$l(X) = (\mathbf{a}_L - z \cdot \mathbf{1}^n) + \mathbf{s}_L \cdot X, \qquad r(X) = \mathbf{y}^n \circ (\mathbf{a}_R + z \cdot \mathbf{1}^n + \mathbf{s}_R \cdot X) + z^2 \cdot \mathbf{2}^n \tag{3}$$

A belső szorzatuk: $t(X) = \langle l(X), r(X) \rangle = t_0 + t_1 X + t_2 X^2$. P elküldi a t_1 és t_2 együtthatók commitment-jeit:

$$T_1 = g^{t_1} h^{\tau_1}, \qquad T_2 = g^{t_2} h^{\tau_2} \tag{4}$$

(ahol τ_1, τ_2 véletlen blinding faktorok). V ezekből nem tudja kiolvasni t_1-et vagy t_2-t.

4. lépés (V $\rightarrow$ P): Második challenge.

V véletlenszerűen választ $x \in \mathbb{Z}_p$-t és elküldi P-nek. Ez lesz a kiértékelési pont a polinomokhoz.

5. lépés (P $\rightarrow$ V): Kiértékelt értékek küldése.

P kiszámítja és elküldi: $\hat{t} = t(x)$, $\tau_x = \tau_2 x^2 + \tau_1 x + z^2 \gamma$ (aggregált blinding faktor), $\mu = \alpha + \rho x$, valamint $\mathbf{l} = l(x)$ és $\mathbf{r} = r(x)$ vektorokat.

6. lépés (V ellenőrzi): Fő verifikáció.

V ellenőrzi, hogy a kapott $\hat{t}$ konzisztens-e a korábban kapott commitment-ekkel:

$$g^{\hat{t}} h^{\tau_x} \stackrel{?}{=} V^{z^2} \cdot g^{\delta(y,z)} \cdot T_1^{x} \cdot T_2^{x^2} \tag{5}$$

A bal oldal a P által állított $\hat{t}$ commitment-je. A jobb oldal az, amit $\hat{t}$-nek lennie kellene ($z^2 v + \delta + t_1 x + t_2 x^2$) az ismert commitment-ekből összerakva. Ha egyeznek, V meggyőződött arról, hogy $t_0 = z^2 v + \delta(y,z)$, ami pontosan a tartomány-feltétel.

7. lépés: Belső szorzat argumentum (logaritmikus tömörítés).

Az $\mathbf{l}$ és $\mathbf{r}$ vektorok közvetlen elküldése $O(n)$ méretű lenne. Ehelyett P és V egy rekurzív protokollt futtatnak: minden lépésben P elküldi az L_j, R_j commitment-eket, V egy x_j challenge-et ad, és a vektorméretet felezik. $\log_2 n$ lépés után V egyetlen multi-exponenciálással ellenőrzi:

$$\mathbf{g}^{a \cdot \mathbf{s}} \cdot \mathbf{h}^{b \cdot \mathbf{s}^{-1}} \cdot u^{a \cdot b} \stackrel{?}{=} P \cdot \prod_{j=1}^{\log_2 n} L_j^{x_j^2} \cdot R_j^{x_j^{-2}} \tag{6}$$

Az aggregált bizonyítás mérete m darab n-bites tartomány-bizonyításra:

$$\underbrace{2(\lceil \log_2 n \rceil + \lceil \log_2 m \rceil) + 4}_{\text{csoportelemek}} + \underbrace{5}_{\mathbb{Z}_p\text{-elemek}} \tag{7}$$

Tehát m bizonyítás összemérete csak $\log(m)$-mel nő – ez teszi a Bulletproofs-t gyakorlatilag használhatóvá a Monero-ban, ahol minden tranzakció tartalmaz range proof-ot.

1.3 RandomX bányászat

A Monero tudatosan CPU-barát PoW algoritmust alkalmaz (jelenleg RandomX [3]), amely ellenáll az ASIC-optimalizálásnak. A RandomX célja, hogy a bányászatot a lehető legigazságosabbá tegye: a hétköznapi számítógépek versenyképesek maradjanak a speciális hardverekkel szemben, megakadályozva a Bitcoinnál tapasztalt centralizációt.

A RandomX működési elve: minden hash-számításhoz egy véletlenszerű programot generál, amelyet végre kell hajtani. Ez a program a következő CPU-képességeket igényli:

- Egész aritmetika (összeadás, szorzás, osztás, bitműveletek).
- Lebegőpontos aritmetika (IEEE 754 double precision).
- Elágazás-előrejelzés (branch prediction) – a program tartalmaz feltételes ugrásokat.
- L3 cache hozzáférés – a program egy 2 GB-os „dataset”-ből olvas véletlenszerű címekről.
- Szuperskalár pipeline kihasználás – az utasítások függőségi lánca úgy van tervezve, hogy a modern CPU-k párhuzamos végrehajtási egységeit kihasználja.

A RandomX két módban működik:

- Fast mode: 2 GB RAM szükséges a dataset tárolásához. Ez a bányászati mód, amelyet a teljes csomópontok használnak.
- Light mode: 256 MB RAM elegendő, de $\approx 6\times$ lassabb. Ezt az ellenőrző csomópontok használják.

Az ASIC-ellenállóság azon alapul, hogy egy ASIC, amely véletlenszerű programokat hajt végre egész és lebegőpontos aritmetikával, elágazásokkal, és nagy memória-hozzáféréssel, lényegében maga is egy általános célú CPU lenne – tehát nem nyújt jelentős előnyt egy hagyományos processzorhoz képest. A GPU-k sem hatékonyak, mert a RandomX programok erősen szekvenciálisak és sok elágazást tartalmaznak, ami ellentétes a GPU-k SIMD architektúrájával.

A dataset minden 2048 blokkönként ($\approx$ 2,8 naponta) újragenerálódik, és a generálás maga is számításigényes (AES, Blake2b hash-ek láncolása), ami megakadályozza, hogy a dataset-et menet közben számolják ki ahelyett, hogy tárolnák.

1.4 Tőzsdei kereskedés és szabályozási problémák

A Monero az anonimitása miatt sajátos helyzetben van a kriptovaluta-tőzsdék világában. A főbb tőzsdék közül jelenleg a következők listázzák az XMR-t: Binance (korlátozásokkal, az EU-ban 2024-ben delistázták), KuCoin, Kraken (egyes régiókban elérhető), Gate.io, Huobi (HTX), MEXC, Bitfinex, Poloniex, TradeOgre és Cake Wallet (decentralizált váltó). A Coinbase soha nem listázta a Monero-t szabályozási aggályok miatt.

A szabályozási problémák a Monero anonimitás-garanciáiból fakadnak:

- KYC/AML megfelelés: a legtöbb joghatóságban a tőzsdéknek ismerniük kell ügyfeleik személyazonosságát (Know Your Customer) és figyelniük kell a pénzmosás-gyanús tranzakciókat (Anti-Money Laundering). A Monero tranzakciók láncelemzése technológiailag nem lehetséges, ami ellentétben áll ezekkel a követelményekkel.

- Travel Rule: a FATF (Financial Action Task Force) előírja, hogy a virtuális eszközök szolgáltatói (VASP-ok) osszák meg a küldő és fogadó adatait egymással. A Monero stealth address-ei miatt ez nem teljesíthető.

- EU MiCA rendelet: a 2024-ben hatályba lépett szabályozás szigorítja az anonim kriptovaluták kezelését, ami több európai tőzsde XMR-delistázásához vezetett.

- Darknet piacok: a Monero a Silk Road utódpiacok (pl. AlphaBay, Dream Market utódok) preferált fizetőeszközévé vált a Bitcoin helyett, ami fokozott hatósági figyelmet von magára.

- IRS jutalom: az amerikai adóhivatal (IRS) 2020-ban 625 000 USD jutalmat tűzött ki a Monero-tranzakciók nyomon követésére képes eszközök fejlesztéséért [4].

A Monero közösség álláspontja szerint az anyagi tranzakciók magánszférája alapvető emberi jog, és az anonimitás technológiája önmagában semleges. A szabályozók ezzel szemben a technológiai lehetetlenséget (a tranzakciók nyomonkövethetetlenségét) rendszerszintű kockázatnak tekintik. Ez a feszültség a kriptovaluták szabályozásának egyik legélesebb nyitott kérdése.

A cryptojacking a PoW bányászat externáliáinak szélsőséges példája: a bányászati költséget (energia, hardver-amortizáció) tudtukon kívül a felhasználókra hárítja, miközben a haszon a támadóé. Ez is alátámasztja azt az érvet, hogy a PoW rendszerek gazdasági ösztönzőstruktúrája visszaélésre csábít.

Hivatkozások

[1] S. Noether, *Ring Confidential Transactions*, Ledger, vol. 1, pp. 1–18, 2016.

[2] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More*, IEEE Symposium on Security and Privacy, pp. 315–334, 2018.

[3] T. Howard et al., *RandomX: ASIC-resistant Proof-of-Work Algorithm*, 2019. `https://github.com/tevador/RandomX`

[4] Internal Revenue Service, *Pilot IRS Will Pay Up to $625,000 for Cryptocurrency Tracing Tools*, IRS Criminal Investigation, Request for Information RFI-CI-20-0006, 2020.