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 MEV: Maximal Extractable Value, front-running és a PBS

A *Maximal (korábban Miner) Extractable Value* (MEV) azt a profitot jelenti, amelyet egy blokkot összeállító szereplő a tranzakciók *beillesztésének, kizárásának és sorrendezésének* szabad megválasztásával kinyerhet – a felhasználóknak fizetett szokásos díjakon felül. Mivel az Ethereumon a nyilvános mempool látható, és a blokkon belüli sorrend monopolisztikusan a javaslattevő (illetve a nevében építő szereplő) kezében van, a tranzakciók *átrendezése* önálló értékforrássá válik. Az MEV kutatási szempontból kiemelten gazdag téma, mert egyszerre érint mikroökonómiát, mechanizmustervezést, hálózatbiztonságot és decentralizációt.

Az MEV mint optimalizációs probléma. Legyen $\mathcal{P}$ a mempoolban elérhető tranzakciók halmaza, és jelölje σ egy blokk *rendezett* tranzakciósorozatát ($\sigma \subseteq \mathcal{P}$, a protokoll korlátai – gas-limit, érvényesség – mellett). A kinyerhető érték:

$$\mathrm{MEV} = \max_{\sigma} \ \Pi(\sigma) \quad \text{feltéve, hogy } \sigma \text{ érvényes és } \sum_{i \in \sigma} g_i \leq G_{\max}, \tag{1}$$

ahol $\Pi(\sigma)$ az építő összprofitja a σ sorrend mellett (saját tranzakciók nyeresége + díjak + borravalók). Az MEV tehát egy *beágyazott kombinatorikus optimalizáció*: az építő a lehető legjövedelmezőbb sorrendet keresi.

Főbb MEV-stratégiák.

- **Arbitrázs**: ugyanazon eszköz áreltéréseinek kihasználása DEX-ek között; jellemzően „hasznos”, mert közelíti az árakat (ökoszisztéma-érték).
- **Likvidációk**: alulfedezett hitelpozíciók likvidálása a likvidációs bónuszért (lásd a lending protokollokat); szintén részben hasznos.

- **Front-running**: egy jövedelmező, még függő (pending) tranzakciót észlelve a támadó egy saját tranzakciót tesz *elé* magasabb prioritással.
- **Back-running**: egy tranzakció *mögé* való beillesztés (pl. egy nagy swap utáni arbitrázs).
- **Sandwich-támadás**: a front- és back-running kombinációja; ez jellemzően tiszta járadékkitermelés (rent extraction) a kiskereskedő kárára.

A sandwich-támadás mechanizmusa és matematikája. Tegyük fel, hogy egy áldozat egy konstans-szorzat ($x \cdot y = k$) AMM-poolban Δx_v mennyiségű X-et akar Y-ra váltani. A támadó a sorrendet így rendezi:

1. **Front-run**: a támadó előbb vásárol Δx_a-t, felhajtva az árat. A pool $(x, y) \to (x + \Delta x_a,\ y - \delta_a)$ állapotba kerül, ahol $\delta_a = \dfrac{y\,\Delta x_a}{x + \Delta x_a}$.
2. **Áldozat ügylete**: az áldozat a már *megemelt* áron hajtja végre a swapjét, azaz kevesebb Y-t kap, mint különben kapott volna – a különbség a támadó megragadott járadékának forrása.
3. **Back-run**: a támadó visszaadja a frissen szerzett Y-t, és a mesterségesen megemelt áron realizálja a profitot.

A támadó nettó profitja (díjak nélkül) a be- és kilépés közti árkülönbségből adódik; az áldozat vesztesége lényegében a saját swapjén elszenvedett *extra slippage*. Az áldozat ezt egy *csúszási tolerancia* (slippage tolerance, s) megadásával korlátozhatja: a tranzakció visszafordul (revert), ha a kapott mennyiség $< (1 - s) \cdot \Delta y^{\text{ideális}}$. Minél szűkebb s, annál kevésbé profitálhat a sandwich – de annál gyakrabban hiúsul meg a saját ügylet.

Empirikus nagyságrendek. Mérések szerint a sandwich-támadások gyakoriak – egyes elemzések nagyságrendileg *blokkonként* átlagosan egy körüli előfordulást jeleznek. Az összesített (lifetime) MEV-nek becslések szerint hozzávetőleg 35%-a arbitrázs, 30%-a sandwich, 25%-a likvidáció és 10%-a egyéb kategória – vagyis a kitermelt érték jelentős része (a sandwich) tiszta járadék a kiskereskedő rovására, míg az arbitrázs és a likvidáció részben ökoszisztéma-hasznot teremt. (A konkrét arányok forrásonként és időszakonként erősen változnak.)

Proposer–Builder Separation (PBS). A naiv modellben a blokk javaslattevőjének (proposer) kellene a bonyolult MEV-optimalizációt is elvégeznie, ami erős *centralizációs* nyomást teremt (a legjobb optimalizáló nyer). A PBS ezt a két szerepet szétválasztja:

$$\underbrace{\text{Builder}}_{\text{összeállítja a legértékesebb blokkot}} \xrightarrow{\text{ajánlat / licit}} \underbrace{(\text{Relay})}_{\text{közvetít, elrejti a tartalmat}} \to \underbrace{\text{Proposer / validátor}}_{\text{a legmagasabb licitet választja}}.$$

- A **builderek** versenyeznek a legjövedelmezőbb (legtöbb MEV-et tartalmazó) blokk összeállításáért, és egy licitet (bid) ajánlanak a javaslattevőnek.
- A **proposer** (a sorsolt validátor) nem látja a blokk teljes tartalmát a választáskor, csak a licit nagyságát – és a legmagasabbat választja.

- A gyakorlatban ezt egy protokollon *kívüli* rendszer, az **MEV-Boost** valósítja meg *relay*-eken keresztül, amelyek a builder és a proposer közt közvetítenek, és garantálják az atomi kifizetést.

A PBS célja, hogy a MEV-ből származó előnyt *demokratizálja*: egy átlagos otthoni validátor is hozzájut a profi builderek által termelt értékhez, anélkül hogy magának kellene MEV-et optimalizálnia. Formálisan, ha V_{bid} a nyertes licit és R a builder megtartott maradéka, akkor a kinyert MEV felosztása MEV $\approx V_{\text{bid}} + R$, ahol a tapasztalat szerint a licit (azaz a proposer része) a blokkérték *nagy hányadát* teszi ki.

A blokképítői piac és az ePBS. A jelenlegi MEV-Boost rendszerben a javaslattevő (proposer) a blokképítési feladatot külső blokképítőre (builder) bízhatja. A blokképítő tranzakciókat gyűjt, szimulálja a lehetséges sorrendeket, és olyan blokkot állít össze, amely a protokollszabályok betartása mellett nagy bevételt termel. A blokképítők ajánlatot tesznek a javaslattevőnek; az ajánlat a blokkért cserébe ígért kifizetés. A közvetítő (relay) a rejtett blokkajánlat és a teljes blokk átadásának menetét koordinálja. Ez lehetővé teszi, hogy kisebb validátorok is hozzáférjenek a hivatásos blokképítők optimalizálásához, de a közvetítő megbízhatóságára és rendelkezésre állására támaszkodik.

A blokképítői piac nem feltétlenül válik versengővé pusztán attól, hogy több szereplő adhat be ajánlatot. Egy empirikus vizsgálat szerint a piaci részesedés együtt jár a változatosabb tranzakcióforrással, a nyereségességet pedig különösen segíthetik a kizárólagos tranzakciós kapcsolatok. Ez önmagát erősítő előnyt hozhat létre: a nagyobb blokképítő több egyedi tranzakcióhoz jut, ezért jobb ajánlatot adhat, így tovább növelheti részesedését [1]. A koncentráció csökkentheti a versenyt, és növeli annak kockázatát, hogy néhány szereplő tranzakciókat hagy ki vagy cenzúráz.

Az ePBS (protokollba épített javaslattevő–blokképítő szétválasztás) a szerepek szétválasztását a konszenzusprotokoll részévé tenné. Az EIP-7732 javaslatában a javaslattevő egy aláírt blokkérték-ajánlatot rögzít, a blokképítő pedig később felfedi a hozzá tartozó végrehajtási blokkot. A javaslat protokollszintű kifizetési és ellenőrzési mechanizmust is leír, amely mérsékelheti a közvetítőbe vetett bizalom szükségességét. Az EIP felülvizsgálat alatt álló javaslat, nem az Ethereum már bevezetett funkciója [2].

Titkosított mempool és küszöbös titkosítás. A nyilvános mempoolban a blokkba még be nem került tranzakciók tartalma olvasható. Titkosított mempoolban a beküldő titkosítja a tranzakciót, így a blokképítő a felfedés előtt nem látja annak részleteit. Küszöbös titkosításnál a visszafejtési kulcsot több résztvevő között osztják szét. Ha a rendszer n kulcsőrt használ, és a visszafejtéshez legalább k résztvevő együttműködése szükséges, akkor egyetlen kulcsőr önmagában nem tudja idő előtt felfedni a tranzakciót. A küszöb elérésekor a résztvevők kulcsrészleteket adnak ki, amelyekből a tranzakció visszafejthető [3].

Az egyik változat előbb rögzíti a tranzakciók sorrendjét vagy az azokat tartalmazó blokkot, és csak utána teszi olvashatóvá a tranzakciókat. Ez csökkentheti a függő ügyletek alapján végrehajtott előrefutást és szendvicstámadást. A titkosítás azonban önmagában nem garantálja a tranzakció bekerülését, nem szüntet meg minden arbitrázst, és nem akadályozza meg a visszafejtés utáni sorrendezési előnyt. További kockázat, hogy a kulcsőrök összejátszanak, vagy elegendő számú résztvevő visszatartja a kulcsrészletét. Ezért a kulcsőri kör összetétele, a visszafejtés időzítése és a kiesések kezelése a biztonsági modell része.

Gyertyaárverések a blokképítésben. A gyertyaárverés olyan nyílt licitálású aukció, amelynek lezárási időpontja előre nem ismert vagy véletlenszerű. A név a történeti gyakorlatra utal, ahol egy gyertya kialvása jelezte a licit végét. Blokképítési változatában a résztvevők egymás ajánlatait látva emelhetnek, de nem tudják pontosan, meddig van idejük. Ez mérsékelheti az utolsó pillanatban történő ajánlat-leütést, ugyanakkor a kiszámíthatatlan lezárás versenyelőnyt adhat a gyorsabb résztvevőknek. Az Ethereum blokképítői piacán vizsgált gyertyaárverés kutatási aukcióforma, nem a jelenlegi protokoll kötelező része [4].

Előzetes tranzakció-visszaigazolások. Az előzetes visszaigazolás (preconfirmation, röviden preconf) a blokk végleges közzététele előtt adott ígéret arra, hogy egy tranzakció egy későbbi blokkba bekerül, vagy meghatározott feltétellel végrehajtódik. Az ígéretet jellemzően egy javaslattevő vagy az általa megbízott szereplő írja alá. A felhasználó így a szokásos blokkvárakozásnál korábban kaphat visszajelzést; az előzetes visszaigazolás azonban önmagában nem konszenzusos véglegesség. A hitelességet letét, büntetési szabály vagy más gazdasági biztosíték támogathatja. A vállalás pontosan rögzítheti, hogy csak a bekerülést, vagy a tranzakció adott sorrendben történő végrehajtását ígéri [5, 6].

Cenzúra-ellenállás és a tranzakciók kikényszerített bevétele. Cenzúráról beszélünk, ha egy blokképítő vagy javaslattevő egy érvényes, megfelelő díjú tranzakciót szándékosan kihagy. Egyetlen blokk kihagyása még nem feltétlenül akadályozza meg a tranzakció későbbi bekerülését, de a tartós kihagyás vagy a blokképítők összpontosulása komoly hozzáférési problémát okozhat. A szolgáltatók közti verseny segíthet, de önmagában nem biztosítja, hogy minden tranzakció bekerüljön.

Az egyik vizsgált megoldás a befogadási lista (inclusion list): egy validátori bizottság összeállítja a mempoolból látott, beillesztendő tranzakciók listáját. Az EIP-7805-ben leírt FOCIL-terv szerint a blokképítőnek be kell emelnie a listákon szereplő, érvényes tranzakciókat; a következő kör validátorai pedig csak akkor szavaznak a blokkra, ha ez teljesült. A terv a tranzakciók időbeni bekerülését segítené, de maga az EIP jelenleg tervezet, nem aktív Ethereum-szabály [7].

A titkosított mempool és a befogadási lista eltérő kérdésre válaszol: az előbbi a tranzakció tartalmát rejtheti el a korai megfigyelők elől, az utóbbi a kihagyás ellen adna protokollszintű garanciát. Együtt is alkalmazhatók, de a titkosított tranzakciók érvényességének ellenőrzése és a visszafejtés időzítése ilyenkor külön tervezési feladat.

Hivatkozások

[1] B. Öz, D. Sui, T. Thiery, F. Matthes, *Who Wins Ethereum Block Building Auctions and Why?*, Advances in Financial Technologies, 2024. arXiv:2407.13931. https://arxiv.org/abs/2407.13931

[2] Ethereum Improvement Proposals, *EIP-7732: Enshrined Proposer-Builder Separation*. https://eips.ethereum.org/EIPS/eip-7732

[3] Shutter Network, *How Shutter API Works: threshold encryption and commit-and-reveal*. https://docs.shutter.network/docs/protocol/api/how_it_works

[4] J. Schlegel, *Why searchers and builders like candle auctions (and why it matters for the builder market post-Glamsterdam)*, Ethereum Research, 2026. https://ethresear.ch/t/26211

[5] J. Drake, *Based preconfirmations*, Ethereum Research, 2023. https://ethresear.ch/t/based-preconfirmations/17353

[6] A.-P. Stouka et al., *SoK: Preconfirmations*, arXiv:2510.02947, 2025. https://arxiv.org/abs/2510.02947

[7] Ethereum Improvement Proposals, *EIP-7805: Fork-choice enforced Inclusion Lists (FOCIL)*. https://eips.ethereum.org/EIPS/eip-7805