

Kriptovaluták elméleti hátttere

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. október 15.

1 Ethereum DeFi ökoszisztéma

1.1 Real-World Assets (RWA) az Ethereum ökoszisztémában

Az RWA (Real-World Assets) az Ethereum ökoszisztéma egyik legfontosabb aktuális trendje. Lényege, hogy valamilyen valós eszköz tulajdonjogát vagy követelését egy blokkláncon lévő token reprezentálja. Az Ethereum Foundation definíciója szerint az RWA olyan token, amely egy meglévő vagyoni elemet (ingatlan, kötvény, arany, részvény, hitelportfólió stb.) képvisel a blokkláncon.

Mit tokenizálnak? Tipikus RWA-k: államkötvények (US Treasury Bills), pénzpiaci alapok, vállalati kötvények, magánhitelek (private credit), ingatlanok, részvények és árupiaci termékek (pl. arany). 2026 elején már hat eszközkategória lépte át egyenként az 1 milliárd dolláros on-chain értékhatárt.

Hogyan működik? Például egy 100 millió eurós kötvényalap esetén: az alapkezelő létrehozza a jogi struktúrát, kibocsát 100 000 000 darab tokenet Ethereumon, ahol egy token egy eurónyi részesedést testesít meg. A tokenek 24/7 átadhatók, kereskedhetők vagy akár DeFi-protokollokban fedezetként használhatók. Formálisan egyetlen token értéke $p_{\text{token}} = V/N$, ahol V az alap nettó eszközértéke (NAV), N pedig a kibocsátott tokenek száma.

Miért fontos az Ethereum? Az Ethereum vált a vezető RWA-platformmá, mert fejlett okosszerződés-rendszerrel és nagy likviditású stablecoin-ökoszisztémával rendelkezik, intézményi szereplők is elfogadják, Layer-2 hálózatai pedig olcsó tranzakciókat biztosítanak. 2026 közepén az Ethereumon tartott tokenizált RWA-érték mintegy 16,6 milliárd dollár volt, ami a teljes on-chain RWA-piac kb. 52,85%-át tette ki. A legnagyobb intézményi projektek közül több is Ethereumon fut: *BlackRock BUIDL* (~2,68 Mrd USD), *Franklin Templeton BENJI* (~1,0 Mrd USD), *Ondo Finance* (USDY ~2,24 Mrd USD) és *Superstate USTB* (~967 M USD).

Kapcsolat a DeFi-vel. A klasszikus DeFi-ben a fedezetek jellemzően kriptoeszközök (ETH, BTC, stablecoinok). Az RWA-k révén azonban tokenizált államkötvény lehet fedezet, tokenizált pénzpiaci alap lehet likviditási eszköz, és valós kamatot termelő eszközök kerülnek a DeFi-be (a tokenizált T-Bill termékek 2026-ban jellemzően 3,4–3,6% éves hozamot kínáltak). Ez a DeFi és a hagyományos pénzügyek (TradFi) konvergenciáját jelenti.

Biztonsági és bizalmi probléma. Míg ETH esetén a tulajdonjogot maga a blokklánc garantálja, RWA esetén a token mögött egy külső jogi követelés áll. Ezért meg kell bízni a letétkezelőben, az eszközkibocsátóban, a jogi struktúrában és az auditorokban. Az RWA tehát nem szünteti meg teljesen a közvetítőket, hanem digitálisabbá és automatizáltabbá teszi őket.

Méret. 2026-ban a tokenizált RWA-piac már több tízmilliárd dollárra nőtt: több forrás szerint a teljes on-chain RWA-állomány 34–46 milliárd USD nagyságrendű, és ennek legnagyobb része Ethereumon található.

1.2 Automated Market Makerek (AMM) a DeFi-ben

Az Automated Market Maker (AMM) a decentralizált pénzügyek (DeFi) egyik alapvető építőköve. A hagyományos, ajánlati könyvre (order book) épülő tőzsdékkal szemben az AMM nem párosítja össze a vevőket és eladókat, hanem egy *likviditási medence* (liquidity pool) és egy determinisztikus árazási képlet alapján teszi lehetővé a kereskedést. A likviditást a felhasználók (likviditásszolgáltatók, LP-k) biztosítják, és cserébe a kereskedési díjak egy részét kapják.

A konstans szorzat modell. A legegyszerűbb árazási szabály a *constant product* (konstans szorzat) invariáns. Legyen x és y a medencében lévő két eszköz mennyisége. Az invariáns:

$$x \cdot y = k, \quad (1)$$

ahol k konstans a kereskedés során. A pillanatnyi ár (az Y eszköz X -ben kifejezve):

$$P = \frac{y}{x}. \quad (2)$$

Ha egy kereskedő Δx mennyiségű X eszközt ad be, akkor a kapott Δy mennyiségre az invariáns megőrzése miatt:

$$(x + \Delta x)(y - \Delta y) = k \implies \Delta y = y - \frac{k}{x + \Delta x} = \frac{y \Delta x}{x + \Delta x}. \quad (3)$$

A $\gamma = 1 - f$ díjtényezővel (ahol f a kereskedési díj, pl. $f = 0,003$, azaz 0,3%) a tényleges kimenet:

$$\Delta y = \frac{y \gamma \Delta x}{x + \gamma \Delta x}. \quad (4)$$

Árhatás (slippage). Mivel a görbe nemlineáris, nagyobb ügyletek egyre kedvezőtlenebb átlagárat kapnak. A végrehajtási átlagár $\bar{P} = \Delta y / \Delta x$ mindig rosszabb, mint a kezdeti marginális ár $P = y/x$, és az eltérés (slippage) a $\Delta x/x$ aránnyal nő. Határesetben $\Delta x \rightarrow 0$ mellett $\bar{P} \rightarrow P$.

Likviditásslolgáltatás és impermanens veszteség. Az LP-k x és y eszközt helyeznek be a pillanatnyi ár arányában. Ha az ár P_0 -ról P_1 -re változik, és $r = P_1/P_0$ az árarány, akkor a konstans szorzat modellben az LP pozíció értéke a pusztán tartáshoz (HODL) képest kisebb lesz; ez az *impermanens veszteség* (impermanent loss, IL):

$$IL(r) = \frac{2\sqrt{r}}{1+r} - 1 \leq 0. \quad (5)$$

Például $r = 2$ (az ár megduplázódik) esetén $IL \approx -5,7\%$, $r = 4$ esetén $IL \approx -20\%$. Az IL-t a felhalmozott kereskedési díjak ellensúlyozhatják.

Fontosabb AMM-görbetípusok.

- **Konstans szorzat** ($x \cdot y = k$): univerzális, bármilyen árra működik, de a likviditás egyenletesen oszlik el 0 és ∞ között, így tőkehatékonysága alacsony.
- **Konstans összeg** ($x + y = k$): nulla slippage, de a tartalék kimeríthető és az ár fixen 1 marad – önmagában instabil, ritkán használt.
- **Stablecoin / hibrid görbék** (pl. a StableSwap-típus): a konstans összeg és konstans szorzat kombinációja, amely az 1:1 ár közelében alacsony slippage-t ad hasonló értékű eszközök (stablecoinok) között.
- **Koncentrált likviditás**: az LP-k egy $[P_a, P_b]$ árintervallumra összpontosíthatják a tőkéjüket. A likviditás L paraméterrel kifejezve egy pozíció virtuális tartalékait a $(x + L/\sqrt{P_b})(y + L/\sqrt{P_a}) = L^2$ összefüggés írja le, ami az adott sávon belül úgy viselkedik, mint a klasszikus $xy = k$, de jóval nagyobb tőkehatékonysággal.

Előnyök és kockázatok. Az AMM-ek fő előnye a *permissionless*, folyamatos (24/7) likviditás és az, hogy bárki lehet likviditásslolgáltató. Fő kockázataik: az impermanens veszteség, a nagy ügyletek slippage-e, az árfolyam-manipuláció (pl. oracle-támadások) és a mögöttes okoszerződés hibái. A DeFi-ben az AMM-ek a decentralizált tőzsdék (DEX-ek) több tíz milliárd dolláros összlikviditásának (TVL) nagy részét adják.

1.3 DeFi hitelezési protokollok: Morpho és társai

A hitelezési (lending/borrowing) protokollok a decentralizált pénzügyek (DeFi) másik alappillére adják az AMM-ek mellett. Lényegük, hogy a felhasználók túlfedezett (overcollateralized) kölcsönöket vehetnek fel: eszközt helyeznek letétbe fedezetként, és egy másik eszközt vesznek kölcsön ellene. A kamatlábakat nem egy központi szereplő, hanem egy determinisztikus, kihasználtságfüggő (utilization-based) kamatmodell állapítja meg. 2026-ban a teljes DeFi-hitelezési állomány (TVL) rekordot döntött, kb. 55 milliárd dollár körül tetőzött, és a top tíz protokoll a betétek nagyjából 88%-át koncentrált.

Alapfogalmak: kihasználtság és kamatmodell. Legyen egy piacon S a teljes kínálat (supply) és B a kölcsönvett összeg (borrows). A *kihasználtság* (utilization):

$$U = \frac{B}{S}, \quad 0 \leq U \leq 1. \quad (6)$$

A kölcsönzési kamatláb r_b jellemzően szakaszosan lineáris (törött vonalú) függvénye U -nak egy U^* „töréspont” (kink) körül:

$$r_b(U) = \begin{cases} r_0 + \frac{U}{U^*} m_1, & U \leq U^*, \\ r_0 + m_1 + \frac{U - U^*}{1 - U^*} m_2, & U > U^*, \end{cases} \quad (7)$$

ahol r_0 a báziskamat, m_1 a töréspontig vett meredekség, $m_2 \gg m_1$ pedig a meredek „büntető” szakasz, amely U^* fölött gyorsan emeli a kamatot, hogy likviditást vonzzon vissza. A betéti (supply) kamat ebből:

$$r_s = U \cdot r_b \cdot (1 - \phi), \quad (8)$$

ahol ϕ a protokoll által levont tartalékhányad (reserve factor). Mivel $U \leq 1$, mindig $r_s \leq r_b$, és a kettő közti rés (spread) a protokoll és a kihasználatlan tőke „ára”.

Egészségi faktor és likvidáció. Egy pozíció biztonságát az *egészségi faktor* (health factor) méri. Ha a fedezet értéke C , a likvidációs küszöb (liquidation threshold, LT) pedig a maximálisan kölcsönvehető hányadot adja a fedezet értékéhez képest, akkor adósság D mellett:

$$\text{HF} = \frac{C \cdot \text{LT}}{D}. \quad (9)$$

Amíg $\text{HF} > 1$, a pozíció egészséges; ha $\text{HF} \leq 1$, likvidálhatóvá válik, és egy likvidátor diszkonttal (liquidation bonus) megveheti a fedezet egy részét. A felvehető maximális kölcsön felső korlátját a maximális hitel/fedezet-arány (Loan-to-Value, LTV, illetve izolált piacoknál LLTV – liquidation LTV) szabja meg:

$$D \leq \text{LTV} \cdot C. \quad (10)$$

Két architektúrális iskola.

- **Megosztott (pooled) piacok:** minden eszköz egyetlen, governance által kezelt közös medencébe kerül, közös kockázati paraméterekkel. Egyszerű és mély likviditású, de egy rosszul listázott eszköz az egész poolt veszélyeztetheti.
- **Izolált (modular) piacok:** bárki létrehozhat egy önálló piacot egyedi fedezettel, oracle-lel, LLTV-vel és kamatmodellel. A kockázat piaconként elkülönül, cserébe több utánajárást igényel. Erre épülnek a *kurátor*-vezérelt *vaultok*, amelyek a betéteket több izolált piac között osztják szét.

A peer-to-peer illesztés (Morpho modellje). A hitelezési protokollok fölé épülő optimalizáló réteg (pl. a Morpho eredeti modellje) igyekszik közvetlenül párosítani a hitelezőket és a kölcsönvevőket. Ha egy betét P2P-illesztésben van, a felek a r_b és r_s közötti rés egy közbenső $r_{p2p} \in [r_s, r_b]$ kamattal kapják: a hitelező többet keres, a kölcsönvevő kevesebbet fizet, mint a mögöttes poolban. Illesztetlen tőke esetén a felhasználó a mögöttes protokoll normál pool-kamatára esik vissza. A gyakorlatban ez tipikusan 0,5–2 százalékpont javulást jelent az illesztett pozíciókon.

Példaprojektek (2026).

- **Aave V3** – a legnagyobb pooled lending protokoll, kb. 17–26 Mrd USD TVL (forrásfüggő), sok láncon és eszközzel.
- **Morpho (Blue)** – izolált piacok + kurátor-vaultok; kb. 9–11 Mrd USD nagyságrendű állomány, erős növekedéssel.
- **Spark** (a Sky / korábbi MakerDAO hitelezési ága) – kb. 4,9–6,8 Mrd USD, szorosan kötve a sUSDS megtakarítási rátához.
- **Compound V3** – a klasszikus pooled modell egyik úttörője, kb. 1,4–2,7 Mrd USD, egy-kölcsönésszükség (base asset) piacokkal.
- **Euler V2** – moduláris, engedélyezés nélkül létrehozható piacok.
- **Fluid, Silo, Venus, JustLend** (Tron) – további jelentős, eltérő architektúrájú lending protokollok.

A stablecoin (pl. USDC) betéti hozamok 2026-ban a megbízható platformokon jellemzően a 3,5–9% tartományba estek; a magasabb értékek rendszerint kurátor-vaultokhoz és többletkockázathoz kötődnek.

Kockázatok. A fő kockázatok: oracle-manipuláció (a fedezetérték hibás árazása), likvidációs kockázat volatilis piacon, kamatláb- és kihasználtsági sokkok (bank-run jellegű likviditáshiány magas U mellett), kuratori/listázási hibák az izolált piacokon, valamint okosszerződés-sebezhetőségek. A túlfedezettség (overcollateralization) és a likvidációs mechanizmus együtt védi a protokoll fizetőképességét.

1.4 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:

$$\text{MEV} = \max_{\sigma} \Pi(\sigma) \quad \text{feltéve, hogy } \sigma \text{ érvényes és } \sum_{i \in \sigma} g_i \leq G_{\max}, \quad (11)$$

ahol $\Pi(\sigma)$ az építő összprofitja a σ sorrend mellett (saját tranzakciók nyeresége + díjak + borraivalók). 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 *elő* 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.

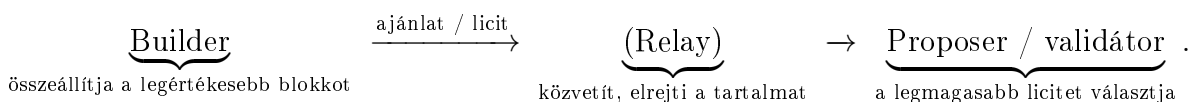
A sandwich-támadás mechanizmusa és matematikája. Tegyük fel, hogy egy áldozat egy konstans-szorzat ($x \cdot y = k$) AMM-poolban Δx_v mennyiségű X -et akar Y -ra váltani. A támadó a sorrendet így rendezi:

1. **Front-run:** a támadó előbb vásárol Δx_a -t, felhajtva az árat. A pool $(x, y) \rightarrow (x + \Delta x_a, y - \delta_a)$ állapotba kerül, ahol $\delta_a = \frac{y \Delta x_a}{x + \Delta x_a}$.
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-hasznos 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:



- 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 $MEV \approx V_{bid} + R$, ahol a tapasztalat szerint a licit (azaz a proposer része) a blokkérték *nagy hányadát* teszi ki.

Nyitott problémák és kutatási irányok. A PBS enyhíti a validátor-szintű centralizációt, de új aggályokat szül: *builder-koncentráció* (néhány builder termeli a blokkok nagy részét), *cenzúra* (mely tranzakciókat zárja ki egy relay), és a MEV-Boost *protokollon kívülisége*. Erre válasz a kutatás és a roadmap több iránya:

- **Enshrined PBS (ePBS)**: a PBS beépítése magába a protokollba, hogy ne kelljen megbízni off-chain relay-ekben.
- **Privát mempoolok / privát tranzakciós csatornák**: a tranzakciók elrejtése a nyilvános mempool elől, hogy ne legyenek front-runolhatók (ugyanakkor ez új, zárt támadási felületet is nyit).
- **Encrypted mempool / threshold-titkosítás**: a tartalom titkosítása a beillesztésig, ami megszünteti a sorrend-alapú kiszípolozás információs alapját.
- **Fair ordering** protokollok: a sorrendezés korlátozása, hogy az átrendezésből származó MEV minimalizálódjon.

Megjegyzendő, hogy az ePBS-sel kapcsolatos elemzések szerint a kinyert blokkérték túlnyomó része (empirikusan 90% felett) a javaslattevőhöz folyik, miközben néhány hatékony builder uralja az aukciót – vagyis a centralizáció–demokratizáció mérlege továbbra is aktív kutatási kérdés.

Hivatkozások