

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: EVM, The Merge, díjmechanizmus és skálázás

1.1 Az Ethereum Virtuális Gép (EVM)

Az EVM egy stack-alapú virtuális gép, amely a smart contract-ok byte-kódját hajtja végre. A végrehajtás állapota egy tuple-ként írható le: (blokk-állapot, tranzakció, üzenet, kód, memória, verem, programszámláló, gas). A blokk-állapot tartalmazza az összes számla egyenlegét és storage-ét. Minden utasítás a kód programszámláló-adik bájttja, és meghatározza, hogyan módosítja a tuple-t. Például az ADD kiveszi a verem felső két elemét, beteszi az összegüket, csökkenti a gas-t 1-gyel, és növeli a programszámlálót. Az SSTORE a verem felső két eleméből az elsőt indexként, a másodikat értéként használja a szerződés storage-ába íráshoz (költsége akár 200 gas).

1.2 Alkalmazások és token-kibocsátás

Az Ethereum legfontosabb hozzájárulása, hogy platformot ad decentralizált alkalmazásoknak. A pénzügyi derivatívák (pl. volatilitás elleni védelem) megvalósításánál a fő kihívás a külső árfolyam-adatok bevitele (oracle probléma). Ennek megoldása oracle smart contract-ok, amelyeket megbízható felek (pl. Chainlink [1]) tartanak karban. Az ERC-20 token szabvány lehetővé teszi, hogy bárki saját kriptovalutát hozzon létre az Ethereumon – ez a korábbi „colored coins” és „metacoins” ötletek természetes továbbfejlesztése. A colored coins (2012) a Bitcoin UTXO-khoz metaadatot rendelt: egy kis értékű Bitcoin tranzakciót „kiszínezték” úgy, hogy az egy részvényt, ingatlant vagy más eszközt reprezentáljon – de a Bitcoin szkriptnyelv korlátozásai miatt ez nehézkes volt és nem támogatta az összetett logikát. A metacoins (pl. Mastercoin/Omni, Counterparty) egy réteget építettek a Bitcoin fölé, ahol a Bitcoin tranzakciók OP_RETURN mezőjébe kódolták a saját protokolljuk utasításait – ez működött, de a Bitcoin hálózat nem értette és nem validálta ezeket a szabályokat. Az Ethereum ERC-20 szabványa ezeket az

ötleteket natívan megoldja: a token-logika smart contract-ként fut az EVM-en, a hálózat maga validálja, és tetszőlegesen összetett szabályok definiálhatók (pl. szavazási jogok, osztalékfizetés, automatikus tőzsdei kereskedés). Az Ethereum monetáris politikája folyamatos kibocsátást alkalmaz (nem fix 21 milliós korlát), de az éves kibocsátási ráta idővel csökken; a 2022-es Merge óta (PoS átállás) az ETH kibocsátás drasztikusan csökkent, és a gas-égetés (EIP-1559 [2]) miatt időnként deflációssá is válik.

1.3 The Merge: átállás proof-of-stake-re

2022. szeptember 15-én az Ethereum sikeresen végrehajtotta a „Merge”-öt: a hálózat proof-of-work konszenzusról proof-of-stake-re állt át. Ez a blokklánc-történelem egyik legnagyobb infrastrukturális változása volt – egy élő, több száz milliárd dollár értékű hálózat konszenzus-mechanizmusának cseréje leállás nélkül.

Az átállást Vitalik Buterin és az Ethereum Foundation kutatócsapata (különösen Danny Ryan, Justin Drake és Dankrad Feist) vezette. Az előzmények évekre nyúlnak vissza: a Beacon Chain (a PoS lánc) 2020 decemberében indult el párhuzamosan a PoW láncsal, és a validátoroknak 32 ETH-t kellett stake-elniük a részvételhez. A Merge során a két lánc összeolvadt: a PoW végrehajtási réteg (execution layer) megőrizte a teljes tranzakciós történetet és az EVM-et, de a blokk-javaslat és véglegesítés a Beacon Chain PoS mechanizmusára állt át.

A Merge motivációi:

- Energiafogyasztás: a PoW Ethereum ≈ 78 TWh/év energiát fogyasztott (Ausztria méretű ország szintje). A PoS-ra átállás után ez $\approx 0,01$ TWh/évre csökkent (99,95%-os csökkenés).
- Centralizáció: a PoW bányászat ASIC-hardvert és olcsó áramot igényelt, ami földrajzi és tőke-centralizációhoz vezetett. A PoS demokratikusabb: bárki validátor lehet 32 ETH-val.
- Skálázhatóság előkészítése: a jövőbeli sharding (adattárhalmazosítás) megvalósítása PoS-t igényel, mert a validátorokat véletlenszerűen kell shard-okhoz rendelni.

A Merge által bevezetett problémák és kompromisszumok:

- MEV-centralizáció: a blokkgyártás (block building) elkülönült a blokk-javaslatlaltól (proposer-builder separation, PBS). A gyakorlatban néhány nagy builder (pl. Flashbots) dominálja a blokkgyártást, ami új centralizációs pont.
- Validátor-centralizáció: a likvid staking protokollok (pl. Lido) a stake jelentős részét koncentrálják, ami de facto centralizációt eredményez.
- Slashing kockázat: a validátorok elveszíthetik stake-jüket szabálysértés vagy technikai hiba esetén.
- Véglegesség késleltetése: a PoS véglegesség $\approx 12,8$ perc (2 epoch), ami lassabb, mint a PoW probabilisztikus megerősítéseinél szokásos 6 blokk (≈ 1 perc).

1.4 Az EIP-1559 díjmechanizmusa és az ETH mint „ultrasound money”

Az EIP-1559 (2021 augusztus, London hard fork) alapjaiban alakította át az Ethereum tranzakciós díjpiacát. A korábbi, első árú aukciós (first-price auction) modellt – amelyben a felhasználók megtippelték a gas-árat, a bányászok pedig a legtöbbet ígérőket választották – egy protokoll által meghatározott *alapidíjra* (base fee) és egy opcionális *borravalóra* (priority fee / tip) cserélte. A reform fő célja a díjak kiszámíthatóbbá tétele és egy automatikus visszacsatolási hurok bevezetése volt.

A fizetett díj felbontása. Egy tranzakció teljes díja a felhasznált gas és a gas-egységenkénti ár szorzata:

$$\text{díj} = g \cdot (b + t), \quad (1)$$

ahol g a felhasznált gas, b az alapidíj (base fee per gas) és t a borravaló (priority fee per gas). A felhasználó egy felső korlátot (maxFeePerGas , $f_{\max}$) és egy maximális borravalót ($\text{maxPriorityFeePerGas}$, $t_{\max}$) ad meg; a ténylegesen fizetett borravaló:

$$t = \min(t_{\max}, f_{\max} - b). \quad (2)$$

A kulcsfontosságú változás a **sorsukban** rejlik: a borravaló (t) a blokk javaslattevőjéhez (validátorhoz) kerül, az **alapidíjat** (b) viszont a protokoll *elégeti* (burn), azaz véglegesen kivonja a forgalomból.

Az alapidíj dinamikája. Az alapidíj minden blokk után a hálózat terheltsége alapján, determinisztikusan igazodik. Legyen G^* a cél-gasmennyiség (gas target) és G_n az n -edik blokk tényleges gasfelhasználása. Az alapidíj frissítése:

$$b_{n+1} = b_n \left(1 + \frac{1}{8} \cdot \frac{G_n - G^*}{G^*} \right). \quad (3)$$

Mivel egy blokk legfeljebb $G_n = 2G^*$ méretű lehet, a $\frac{G_n - G^*}{G^*}$ tényező a $[-1, 1]$ tartományba esik, így az alapidíj blokkonként legfeljebb $\pm \frac{1}{8} = \pm 12,5\%$ -kal változhat:

$$0,875 b_n \leq b_{n+1} \leq 1,125 b_n. \quad (4)$$

Ha a blokk pontosan a céltelítettségen van ($G_n = G^*$, azaz $\approx 50\%$ kihasználtság), az alapidíj változatlan marad. Teli blokkok ($G_n > G^*$) emelik, üresebb blokkok ($G_n < G^*$) csökkentik – ez a visszacsatolás a kihasználtságot a célérték körül stabilizálja.

Példa. Ha $G^* = 15\text{M}$ gas és egy blokk $G_n = 18\text{M}$ gas használ, akkor $\frac{18-15}{15} = 0,2$, így a növekedés $\frac{0,2}{8} = 2,5\%$, és $b_{n+1} = 1,025 b_n$.

Elégetés és nettó kibocsátás: az „ultrasound money” tézis. Az elégetett alapidíj közvetlen deflációs nyomást fejt ki az ETH kínálatára. Jelölje I a validátoroknak kifizetett új ETH kibocsátást (issuance) egy adott időszak alatt, $\mathcal{B}$ pedig az ugyanazon időszak alatt elégetett ETH mennyiségét:

$$\mathcal{B} = \sum_n g_n \cdot b_n, \quad (5)$$

ahol az összegzés a blokkok tranzakcióira fut. A kínálat nettó változása:

$$\Delta \text{Supply} = I - \mathcal{B}. \quad (6)$$

Ha a hálózati aktivitás elég magas ahhoz, hogy $\mathcal{B} > I$, akkor $\Delta\text{Supply} < 0$, azaz az ETH *deflációssá* válik. Mivel a 2022-es „Merge” (az áttérés Proof-of-Workról Proof-of-Stake-re) drasztikusan, nagyságrendileg $\sim 90\%$ -kal csökkentette a kibocsátást (I), a burn-mechanizmus sok időszakban felülmúlja a kibocsátást. Ezt a tulajdonságot nevezi a közösség „ultrasound money”-nak: a kínálat nemcsak korlátozott, hanem a használattal akár aktívan *csökkenhet* is. Formálisan az éves (annualizált) inflációs ráta:

$$\pi = \frac{I - \mathcal{B}}{\text{Supply}}, \quad (7)$$

amely magas aktivitás mellett negatívvá válhat.

Jelentőség és korlátok. Az EIP-1559 három fő előnyt hozott: (1) *kiszámíthatóbb* díjak a determinisztikus alapidj révén; (2) jobb *felhasználói élmény*, mert a pénztárcák pontosabban tudják becsülni a díjat; (3) a burn révén egy *monetáris* csatorna, amely a hálózat használatát közvetlenül összeköti az ETH kínálatával. Fontos korlát, hogy az EIP-1559 nem csökkentette önmagában a díjak *szintjét* – torlódás idején a base fee továbbra is magasra kúszhat –, a tényleges olcsóságot a skálázási megoldások (Layer-2 rollupok, EIP-4844 blobok) hozzák. Az „ultrasound money” tézis érvényessége pedig *feltételes*: csak akkor teljesül, ha a díjégetés tartósan meghaladja a staking-kibocsátást, ami az aktivitás és a staking-arány függvénye.

1.5 Skálázás: Layer-2 megoldások, rollupok és az EIP-4844

Az Ethereum alaprétege (Layer-1, L1) a decentralizáció és biztonság megőrzése érdekében korlátozott áteresztőképességű (nagyságrendileg 10–20 tranzakció/másodperc). A skálázási stratégia lényege, hogy a tranzakciók végrehajtását egy második rétegre (Layer-2, L2) helyezi, miközben a végső biztonságot és a vitarendezést továbbra is az L1 garantálja. A domináns L2-architektúra a *rollup*: sok tranzakciót egyetlen kötegbe (batch) „göngyöl”, a tömörített adatot közzéteszi az L1-en, és csak a végállapotot igazolja ott.

A rollupok alapképlete. Egy rollup gazdaságosságát az adta, hogy a költséges L1-műveleteket amortizálja a kötegben lévő sok tranzakció között. Ha egy köteg N tranzakciót tartalmaz, és az L1-re posztolás összköltsége (adatközzététel + bizonyíték-ellenőrzés) C_{L1} , akkor az egy tranzakcióra jutó L1-költség:

$$c_{tx} = \frac{C_{L1}}{N} + c_{exec}^{L2}, \quad (8)$$

ahol c_{exec}^{L2} az L2-n végzett végrehajtás (olcsó) költsége. Minél nagyobb N , annál kisebb az egy tranzakcióra eső fix L1-költség – innen ered a nagyságrendi díjcsökkenés.

Optimistic vs. ZK-rollup. A két fő rollup-család abban különbözik, *hogyan* bizonyítják az L1 felé, hogy a kötegben lévő állapotátmenet helyes.

- **Optimistic rollup** – alapértelmezésben *érvényesnek feltételezi* a kötegeket, és egy *csalásbizonyíték* (fraud proof) benyújtására nyitva hagy egy vitázási ablakot, jellemzően **7 napot**. Ha senki nem vitatja a határidőn belül, az állapot véglegessé válik. Előny: egyszerűbb, EVM-kompatibilis; hátrány: a vitaablak miatt a kivonás (withdrawal) lassú. *Példák*: Arbitrum, Optimism, Base, World Chain.

- **ZK-rollup (zero-knowledge / validity rollup)** – minden köteghez egy kriptográfiai *érvényességi bizonyítékot* (validity proof, pl. zk-SNARK / zk-STARK) csatol, amelyet az L1 azonnal ellenőriz. Nincs szükség vitaablakra, így a véglegesség órák (nem napok) kérdése. Előny: gyors kivonás, erős kriptográfiai biztonság; hátrány: a bizonyíték generálása számításigényes. *Példák:* zkSync Era, Starknet, Linea, Scroll, Polygon zkEVM.

Formálisan a két modell bizalmi feltevése eltérő. Optimistic esetben a biztonság egy „1-of-N” becsületes feltevésen nyugszik: elegendő *egyetlen* becsületes figyelő (watcher), aki a $T_{\text{challenge}} = 7$ nap alatt benyújtja a csalásbizonyítékot. ZK esetben a helyesség *feltétel nélküli* (a használt kriptográfia helytállósága mellett), mivel az érvénytelen állapotátmenethez tartozó bizonyítékot gyakorlatilag nem lehet előállítani.

Data availability (adat-elérhetőség). A rollupok biztonságának sarokköve, hogy a tranzakciós adat *elérhető* legyen: enélkül senki sem tudná rekonstruálni az L2 állapotát, csalásbizonyítékot készíteni, vagy a saját pozícióját kivonni. Történetileg a rollupok ezt az adatot drága L1-callldata-ként tették közzé – ez volt az L2-díjak legnagyobb tétele. A kérdés tehát: hogyan lehet az adatot elérhetővé tenni *olcsón*, anélkül hogy örökké az L1-en kellene tárolni.

EIP-4844 (proto-danksharding) és a „blobok”. Az EIP-4844 (2024 márc., Dencun) erre vezette be a *blobokat* (binary large objects): egy új, dedikált, *átmeneti* adatcsatornát a rollupok számára. Főbb jellemzők:

- Egy blob $4096 \text{ mezőelem} \times 32 \text{ bájt} \approx 128 \text{ KiB}$ adatot hordoz.
- A blobadat *nem* érhető el az EVM számára (az okosszerződések nem olvassák közvetlenül), és a konszenzus-kliensek csak egy rögzített ideig (≈ 18 nap, 4096 epoch) tárolják, utána törlik (pruning). Ez az *átmenetiség* teszi olcsóvá: a rollupnak csak addig kell az adat elérhető, amíg a csalás- vagy érvényességi bizonyíték letisztul.
- A blobok *saját, külön díjpiac*on árazódnak, az EIP-1559-hez hasonló mechanizmussal, de **exponenciális** alapidíjjal, egy cél-blobszámhoz képest.

A blob-alapidíj frissítése a kumulatív túlfogyasztás függvénye:

$$b_{\text{blob}} = \text{MIN_BASE_FEE} \cdot \exp\left(\frac{E}{\text{UPDATE_FRACTION}}\right), \quad (9)$$

ahol E a cél-blobszámhoz viszonyított *halmozott* eltérés (excess blob gas). Az induló paraméterek szerint a cél 3, a maximum 6 blob volt blokkonként; a 2025. májusi Pectra frissítés a célt 6-ra (max. 9 körül) emelte, és a hosszú távú cél (teljes danksharding) blokkonként akár 64–128 blob, azaz több MiB adatkapacitás.

Hatás és kitekintés. A blobok bevezetése a tipikus L2-tranzakciós díjakat egyik napról a másikra nagyságrendileg **80–95%-kal** csökkentette, mivel a legdrágább tétel (az L1-adatközzététel) sokkal olcsóbbá vált. A roadmap következő lépése a *teljes danksharding* és a *data availability sampling* (DAS), amelyben a node-oknak nem kell a teljes blobadatot letölteniük, csak véletlenszerű mintákat venniük annak igazolására, hogy az adat elérhető – ez teszi majd lehetővé a kapacitás nagyságrendi növelését. 2026-ra az L2-k átvették az

Ethereum tranzakciós forgalmának túlnyomó részét: az optimistic rollupok (Arbitrum, Base, Optimism) vezetnek a lekötött tőke (TVL) és az ökoszisztéma érettsége terén, míg a ZK-rollupok a véglegességi idő és a bizonyíték-ökonómia terén előznek.

Kompromisszumok (összefoglalás). A választás jellemzően a következő tengelyek mentén dől el: *kivonási sebesség* (ZK gyors, optimistic lassú a 7 napos ablak miatt), *EVM-kompatibilitás* (optimistic történetileg egyszerűbb), *költség* (mindkettőt dominálja a blob-díj), és *biztonsági modell* (1-of-N becslésszerű feltevés vs. feltétel nélküli kriptográfiai érvényesség).

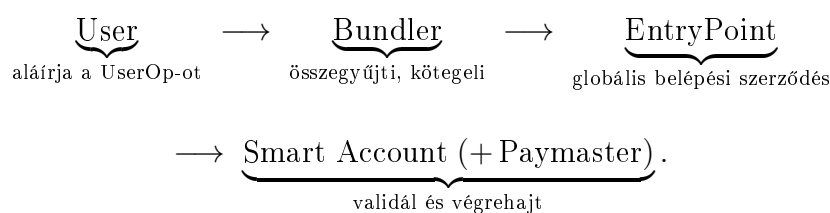
1.6 Account Abstraction: ERC-4337 és EIP-7702

Az Ethereum klasszikus számlamodellje két számlatípust ismer: a külső tulajdonú számlákat (Externally Owned Account, EOA), amelyeket egyetlen privát kulcs vezérel, és a szerződésszámlákat (contract account). A hagyományos EOA-modell három alapvető korlátja: (1) minden művelet egyetlen privát kulcshoz kötött (nincs multisig, social recovery, költséskorlát a protokoll szintjén); (2) a díjat mindig magának a feladónak kell natív ETH-ban fizetnie; (3) a tranzakciók nem köteghelhetők (batch), és az aláírási séma fixen az ECDSA. Az *Account Abstraction* (AA, számla-absztrakció) célja, hogy a számla *programozható logikát* kapjon – lényegében: a számla legyen okosszerződés, ne pusztán egy kulcs.

Mire ad lehetőséget egy „smart account”?

- **Tetszőleges aláírás-ellenőrzés:** nemcsak ECDSA, hanem pl. passkey (WebAuthn), multisig vagy küszöb-aláírás (threshold).
- **Kötege-tranzakciók (batching):** több művelet (pl. `approve` + `swap`) egyetlen atomi lépésben.
- **Social recovery:** kulcsvesztés esetén megbízottak (guardians) állíthatják vissza a hozzáférést.
- **Költési szabályok:** napi limit, whitelistelt címek, session key-ek.
- **Gas-sponsorálás (gasless UX):** harmadik fél vagy maga az alkalmazás fizeti a díjat, akár ERC-20-ban (pl. stablecoinban).

ERC-4337 – AA a protokollon kívül. Az ERC-4337 (2023 márc. óta élő, hard fork *nélkül*) egy teljesen *párhuzamos tranzakciós rendszert* vezet be. A felhasználó nem közönséges tranzakciót küld, hanem egy `UserOperation` nevű objektumot, amely egy külön mempoolba kerül. A folyamat szereplői és egy egyszerűsített életciklus:



- **UserOperation:** a felhasználói szándékot leíró, aláírt objektum.

- **Bundler:** egy szereplő, aki a mempoolból több `UserOp`-ot egyetlen L1-tranzakcióba kötegel, és beküldi az `EntryPoint`-ba (előlegezve a gas, amit utóbb megtérítenek neki).
- **EntryPoint:** egyetlen, globális, auditált szerződés, amely minden AA-folyamat belépési pontja; két fázist futtat: *validáció* majd *végrehajtás*.
- **Paymaster:** opcionális szerződés, amely elvállalhatja a díjfizetést – ez a gas-sponsorálás alapja (sponsored vagy ERC-20-ban fizetett gas).

Formálisan a Paymaster bevezetésével a díjfizető és a tranzakciót kezdeményező szétválk. Jelölje u a felhasználót, p a paymastert és $g \cdot (b + t)$ a tranzakció teljes díját (az EIP-1559 jelöléssel). Klasszikus EOA esetén a díjat mindig u állja; AA + paymaster esetén a díjat p fizeti az `EntryPoint`-nak, és u felé a visszatérítés történhet akár egy másik eszközben (pl. k darab stablecoin), tetszőleges $k = \rho \cdot g(b + t)$ átváltási szabály szerint, ahol ρ a paymaster árazása.

EIP-7702 – AA magára az EOA-ra (Pectra). Az EIP-7702 (a 2025. májusi Pectra hard fork része) más utat jár be: nem új címre telepít külön szerződést, hanem lehetővé teszi, hogy egy *meglévő* EOA *ideiglenesen* okosszerződés-kódra mutasson – **ugyanazon a címen**. Egy új tranzakciótípus (type 4) egy *delegációs mutatót* állít be:

$$\text{EOA}_{\text{cím}} \xrightarrow{\text{delegate}} \text{kód}_{\text{szerződés}}, \quad (10)$$

így a számla a mutató élettartama alatt úgy viselkedik, mint egy smart account (batching, sponsored gas, custom logika), miközben megőrzi a felhasználó eredeti címét, egyenlegét és előzményeit. Ez a legnagyobb UX-előnye: a több száz millió meglévő EOA *újrategelítés nélkül* kaphat AA-képességeket, és visszavonhatóan.

A két megközelítés viszonya. A két szabvány nem versengő, hanem kiegészítő: 2026-ban egymás mellett élnek.

- **ERC-4337:** protokollon kívüli, dedikált smart-wallet infrastruktúrával (bundler, paymaster mempool). Ideális *célzottan* AA-ra épülő pénztárcákhoz; nem igényelt hard forkot.
- **EIP-7702:** protokollszerű, a meglévő EOA-kat „ébreszti fel” AA-képességekkel, és jól kombinálható az ERC-4337 ökoszisztémával (pl. egy 7702-vel upgradelt EOA tud `UserOperation`-öket futtatni).

UX-forradalom és kockázatok. A gyakorlati hatás jelentős: *gasless* tranzakciók (a felhasználónak nem kell ETH-t tartania), ERC-20-ban (pl. stablecoinban) fizetett díj, egyklikkes köteg-műveletek, passkey-alapú bejelentkezés privátkulcs-kezelés nélkül, valamint social recovery a kulcsvesztés mérséklésére. Ez közelebb hozza a web2-höz hasonló felhasználói élményt. A kompromisszumok: az ERC-4337 extra infrastruktúrát (bundler/paymaster) és némi többlet-gas igényel; az EIP-7702 pedig új támadási felületet nyit (a delegáció rossz célra mutatása, phishing-aláírások), ezért a delegáció tartalmának gondos ellenőrzése és a tárca-/aláíró-szintű biztonság kulcsfontosságú.

Hivatkozások

- [1] S. Ellis, A. Juels, S. Nazarov, *ChainLink: A Decentralized Oracle Network*, 2017.
<https://chain.link/whitepaper>
- [2] V. Buterin, E. Conner, R. Dudley, M. Slipper, I. Norden, A. Bakhta, *EIP-1559: Fee Market Change for ETH 1.0 Chain*, Ethereum Improvement Proposals, 2019.
<https://eips.ethereum.org/EIPS/eip-1559>