

Kriptoaluták 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. október 14.

Tartalomjegyzék

1	Proof-of-spacetime, Chia és Helium	2
1.1	Chia Network	2
1.1.1	A proof-of-space protokoll	2
1.1.2	A két fázis biztonsági garanciái	2
1.1.3	Short Range Replotting Attack	3
1.2	Helium Network	3

1 Proof-of-spacetime, Chia és Helium

A proof-of-spacetime a proof-of-space időbeli kiterjesztése. Ebben az esetben nemcsak azt kell bizonyítani, hogy egy adott pillanatban le van foglalva a tárhely, hanem azt is, hogy folyamatosan fenn van tartva egy adott időintervallum alatt. Ez megakadályozza, hogy valaki gyorsan generálja, majd törölje az adatokat, és csak a kérdés pillanatában tartsa magánál azokat.

A folyamatos tárolás bizonyításának kulcseleme a Verifiable Delay Function (VDF) [1]. A VDF egy olyan függvény, amelynek kiszámítása garantáltan legalább T szekvenciális lépést igényel (nem párhuzamosítható), de az eredmény ellenőrzése gyors. Formálisan: adott egy x bemenet, a VDF kimenetét $y = f^{(T)}(x)$ jelöli, ahol f egy ismételten alkalmazott egyirányú függvény (tipikusan moduláris négyzetreemelés: $f(x) = x^2 \bmod N$). A T iteráció szekvenciális jellege miatt a kimenet nem gyorsítható fel párhuzamos hardverrel – pontosan ennyi idő kell a kiszámításához, függetlenül a rendelkezésre álló processzorok számától.

A proof-of-spacetime [2] protokollban a VDF-et arra használják, hogy időbélyegeket fűzzenek a tárolt adatokhoz: a résztvevőnek rendszeres időközönként le kell futtatnia egy VDF-et a tárolt adatokon, és az eredményt be kell nyújtania bizonyítékként. Mivel a VDF kiszámítása a megadott T idő alatt nem rövidíthető le, a résztvevő nem tudja az adatokat törölni és az ellenőrzés pillanatában újragenerálni. A VDF kimenete bizonyítja, hogy az adatok az egész időintervallum alatt rendelkezésre álltak.

1.1 Chia Network

A Chia Network [3] a proof-of-space és a proof-of-time (VDF) kombinációját alkalmazza konszenzus-mechanizmusként. Az alapötlet az, hogy a felhasználók nagy mennyiségű fel nem használt lemezterülettel rendelkeznek, amelyet a blokklánc biztosítására lehetne használni anélkül, hogy jelentős energiát pazarolnának. A marketingereje ennek az hogy ez sokkal kevesebb elektrom áramot igényel mint a PoW.

1.1.1 A proof-of-space protokoll

A Chia proof-of-space protokollja két fázisból áll. Az első fázisban (inicializálás, „plotting”) a bizonyító P létrehoz egy F fájlt („plot”), amelynek mérete N . Ez az inicializálási folyamat kvázilineáris N -ben, tehát a bizonyítónak jelentős számítási munkát kell végeznie egyszer, a fájl létrehozásakor. A hitelesítő V ezzel szemben csak egy kis állapotot tárol.

A Chia Network protokolljában a bizonyító invertálja f -et és letárolja, majd kiszámítja g -t, amelynek argumentumába f inverzét is bele kell építeni. Az ellenőrzés során V elküld egy y értéket, és P -nek vissza kell adnia az x és x' értékeket, amelyek igazolják a tárolást. A g függvényt előre irányban sem könnyű kiszámítani adott x -re, mert ehhez invertálni kell f -et – tehát a Hellman-féle rövidítés nem alkalmazható hatékonyan.

1.1.2 A két fázis biztonsági garanciái

A második fázisban (bizonyítási fázis) V több kérdést intéz P -hez, akinek pedig igazolni kell hogy tárolja az F fájlt. A biztonsági követelmény kimondja, hogy egy csaló bizonyító P' , aki csak egy F' méretű fájlt tárol (ahol $|F'| \ll N$), vagy elbukik a bizonyítás során, vagy jelentős számítási kapacitást kell befektetnie – ideális esetben legalább annyit, amennyibe az F fájl teljes tárolása (vagy újraszámolása) kerülne. Ha megpróbálja

rekonstruálni F -et a korábbi kommunikáció alapján, az ugyanolyan költséges, mint ha egyszerűen tárolta volna.

1.1.3 Short Range Replotting Attack

A Chia rendszerben ismert támadási lehetőség a short range replotting attack. Ennek során a támadó elkezd a plotting folyamatot egy signage point kiadása után, és befejezi a plot létrehozását az infusion point előtt, majd törli a plotot. Mivel a signage point és a plot ID együtt határozza meg a plot filtert, a támadó mindig tud olyan plot ID-t választani, amely átmegy a 512-es filteren – ezzel effektíve 512 plot-nyi (≈ 51 TiB) tárhelyet szimulál egyetlen géppel. A Chia eredeti konszenzusa (egy signage point per 10 perces sub-slot) sebezhető volt ezzel a támadással, hiszen elég volt 10 percnél gyorsabban plotolni. Az új konszenzus 64 signage pontra növelte a sűrűséget (9,375 másodpercenként egy), és az infusion point-ot 3–4 signage pontra helyezte a signage point után. Ez azt jelenti, hogy a támadó számára a minimális konzisztens időablak 28,125 másodperc ($3 \times 9,375$ s), a hálózati késleltetést is figyelembe véve a gyakorlatban ≈ 25 másodperc alatt kellene plotot generálni. Fontos megjegyezni, hogy ez nem klasszikus támadás (a „támadó” nem tud csalni a hálózattal), hanem a rendszert proof-of-work jellegűvé alakítaná – és a Chia tervezésének célja pont ennek megakadályozása volt.

1.2 Helium Network

A proof-of-coverage (PoC) a Helium hálózat [4] konszenzus-mechanizmusa, amely a fizikai világ egy mérhető tulajdonságát, a rádiófrekvenciás (RF) lefedettséget használja a konszenzus alapjául. Míg a PoW számítási munkát, a PoS tőkét, a PoSpace tárhelyet igényel, addig a PoC azt bizonyítja, hogy egy eszköz (Hotspot) valódi vezeték nélküli lefedettséget biztosít egy adott földrajzi területen.

Az algoritmus az RF jelek fizikai terjedési tulajdonságaira épül:

- Az RF jelnek korlátozott fizikai terjedési tartománya van.
- A jelerősség a távolság négyzetével fordítottan arányos (fordított négyzetes törvény): $P_r \propto 1/d^2$.
- Az RF jel a fénysebességgel terjed, tehát a terjedési késleltetés elhanyagolható a hálózati késleltetéshez képest.

A szabadtéri terjedési modell ($P_r \propto 1/d^2$) azonban idealizált esetet ír le. Valós, különösen városi környezetben a vett jelteljesítmény a $P_r \propto 1/d^n$ összefüggést követi, ahol a terjedési kitevő tipikusan $n \in [2, 4]$ értéket vesz fel az árnyékolás és a többutas terjedés hatására. Ez a bizonytalanság egyúttal a PoC egyik gyenge pontja is. A jelerősség-mintázatok természetes szórása mozgásteret ad a csalási kísérleteknek, amelyeket a hálózat statisztikai modellekkel igyekeznek kiszűrni.

A PoC protokoll a következőképpen működik. A hálózat véletlenszerűen kiválaszt egy Hotspotot kihívó (challenger) szerepre. A kiválasztás az előző blokkhashból származtatott pszeudovéletlen értéken alapul. Ez nem teljesen manipulálhatatlan. Elméletileg a blokkgyártó különböző tranzakció-összetételeket próbálgatva (grinding) befolyásolhatná a hash értékét, ám a manipuláció költsége (a blokkjutalom elvesztése és a késleltetés) nagyságrendekkel meghaladja az egyetlen kihívás megnyeréséből származó hasznot, így gazdaságilag elvileg nem racionális. A kihívó egy titkosított kihívást

(challenge) küld egy másik Hotspotnak (a bizonyítónak, challengee). A bizonyítónak RF jellel kell válaszolnia, amelyet a környező Hotspotok (tanúk, witnesses) fognak és jelentenek a hálózatnak. A tanúk által jelentett jelerősség (RSSI) és a válaszidő alapján a hálózat eldönti, hogy a bizonyító valóban a megadott helyen üzemel-e, és valódi lefedettséget biztosít-e.

A PoC biztonsága azon alapul, hogy az RF jelterjedés fizikai törvényeit nem lehet szoftveresen hamisítani. Ha két Hotspot túl messze van egymástól, a jel nem éri el a másikat; ha túl közel vannak egymáshoz (például ugyanabban a szobában), a jelerősség-mintázat nem felel meg a valós városi vagy vidéki környezetnek. A hálózat statisztikai módszerekkel és gépi tanulással észleli a csalási kísérleteket, például a több, azonos helyen üzemelő Hotspotot, a hamis GPS-koordinátákat vagy az RF jel interneten keresztüli továbbítását.

A Helium hálózat a PoC-ot a jutalmak kiosztására használja: a Hotspotok HNT (Helium Network Token) kriptovalutát kapnak a lefedettség biztosításáért és az adatforgalom továbbításáért. Ez arra ösztönzi a résztvevőket, hogy valódi, hasznos vezeték nélküli infrastruktúrát építsenek, szemben a legtöbb más blokkláncsal, ahol a konszenzus-mechanizmus önmagában nem termel a fizikai világban hasznos mellékterméket. A hálózat 2023-ban a Solana blokkláncra költözött, és a lefedettség-ellenőrzés jelentős részét dedikált ellenőrző (Oracle) szolgáltatások vették át.

A proof-of-coverage tágabb jelentősége, hogy a konszenzus-mechanizmus a fizikai világban is hasznos munkát (useful work) termel: a PoW-tól eltérően, ahol a számítási munka egyetlen célja a konszenzus biztosítása, itt a bizonyított erőforrás maga a valós vezeték nélküli lefedettség. Ezzel a PoC a decentralizált fizikai infrastruktúra-hálózatok (Decentralized Physical Infrastructure Networks, DePIN) egyik korai és meghatározó példája. Ugyanakkor a modell korlátai is figyelemre méltóak: a lefedettség pusztán megléte nem feltétlenül jár együtt tényleges adathasználattal, a token-alapú ösztönzés pedig a hasznosságtól elszakadó, spekulatív eszköztelepítést is eredményezhet.

Hivatkozások

- [1] D. Boneh, J. Bonneau, B. Bünz, B. Fisch, *Verifiable Delay Functions*, Advances in Cryptology – CRYPTO 2018, Lecture Notes in Computer Science, vol. 10991, Springer, pp. 757–788, 2018.
- [2] Filecoin Team, *Proof of Replication and Proof of Spacetime*, Protocol Labs Technical Report, 2017. <https://filecoin.io/proof-of-replication.pdf>
- [3] B. Cohen, K. Pietrzak, *The Chia Network Blockchain*, Chia Network, 2019. <https://www.chia.net/assets/Chia-New-Consensus-0.9.pdf>
- [4] A. Haleem, A. Allen, A. Thompson, M. Nijdam, R. Tuesta, *Helium: A Decentralized Wireless Network*, Helium Systems Inc., 2019. <http://whitepaper.helium.com>