Oktalan okosszerződés – avagy mindig az ember győz?*

Kovács Blanka

Ari Juels:
The Oracle
Talos Press, 2024, p. 288
ISBN: 978-1-945863-86-8

A Satoshi Nakamoto által jegyzett Bitcoin whitepaper megjelenése óta számos könyv és tanulmány jelent meg, amely a blokklánc-technológiáról, kriptopiacról, az azon alapuló technológiai és pénzügyi innovációkról – egyben spekulációkról és csalásokról –, illetve társadalomra gyakorolt hatásaikról szólt. A technológia fejlődését nemcsak szakmai körök, hanem a média is kitüntett figyelemmel követi, így nem meglepő, hogy az irodalmi vénával és élénk fantáziával rendelkezőket is megihlette a téma, az Amazonon számos kripto sci-fi műfajú könyvet találunk.

A 2024 februárjában megjelent *The Oracle* azzal emelkedik ki, hogy egy, a blokklánc világában kiváló szaktekintéllyel bíró professzor tollából (vagy "billentyűzetéből") származik. *Ari Juels* a Cornell Egyetem informatikai tanszékének professzora, egyben az IC3 (*Initiative for CryptoCurrencies and Contracts*) társalapítója és a Chainlink Labs tudományos főmunkatársa. Az írónak nem ez az első kalandozása az irodalom területén: a 2010-ben megjelent techno-thriller Tetraktys című könyvnek társírója. Juels több mint száz széles körben idézett tanulmány szerzője, h-indexe[1] magas. Fő kutatási területe az adatbiztonság, adatvédelem, kriptográfia és blokklánc-technológia.

A regény ötlete három forrásból származik: Juels antik kultúra és matematika iránti szenvedélyéből, egy számára különleges helyszínből és egy 2016-ban publikált tanulmányból. A szerző tanulmányait matematika és latin szakon végezte, a történet

* A jelen kiadványban megjelenő írások a szerzők nézeteit tartalmazzák, ami nem feltétlenül egyezik a Magyar Nemzeti Bank hivatalos álláspontjával.

Kovács Blanka: Magyar Nemzeti Bank, elemző. E-mail: kovacsbl@mnb.hu

[1] H-index, egy olyan mérőszám, amellyel egy kutató tudományos teljesítményét mérik. Minél többen hivatkoznak az adott kutató publikációjára, a h-index annál magasabb. 20–30-as h-index nemzetközileg is elismert teljesítményt jelent. Ari Juels h-indexének értéke 100. https://scholar.google.com/citations?user=uf0D-uoAAAAJ&hl=en

történelmi szála innen ered. A híd mint motívum többször visszaköszön a könyvben, a főhős definíciója alapján a blokklánc-orákulumok hidat képeznek a való világ és a zárt blokklánc-rendszerek között. A főhős egy manhatteni skybridge irodában dolgozik, amit az író skybridge-k iránti rajongása és egy előző irodája inspirált. A regény központi ötletét egy publikáció ihlette, amely az okosszerződések és hitelesített adatforrások (*blockchain oracles*) bűnügyi célra történő lehetséges felhasználását vizsgálta. A thriller célja a szórakoztatás mellett a figyelemfelhívás, hogy a mesterséges intelligenciával kombinált blokklánc-megoldások milyen történeteket szülhetnek.

A könyv cselekménye onnan indul el, hogy egy blokklánc-vállalatnál dolgozó szoftverfejlesztő „gonosz" okosszerződés (*rogue smart contracts*) célpontjává válik. A nyílt forráskódot egy Delphian nevű szervezet teszi közzé az interneten, váltságdíjat tűznek a főhős fejére, mert az állítólag nem tisztelte, „megszentségtelenítette" az ókori görög istent, Apollót. Tekintettel az interneten lévő nagy mennyiségű információra, ez akár rossz vicc is lehet. Amikor azonban az első célpont valóban gyilkosság áldozata lesz, a szerződés aktiválódik, és a váltságdíjat valaki valóban felveszi, az már az FBI figyelmét is felkelti.

A blokklánc-technológia – a főhős szerint – koncepcionálisan nem bonyolult, úgy kell elképzelni, mint egy digitális faliújságot (*digital bulletin board*), amely mindenki számára hozzáférhető. Fő tulajdonságai: a tranzakciók gyakorlatilag megmásíthatatlanok, harmadik fél által verifikálhatók, azaz transzparensek. A gyökeres változást az jelenti, hogy okosszerződéseket lehet futtatni rajta. Ezek az okosszerződések (*smart contracts*) szintén megváltoztathatalanok, és nem ellenőrzi őket egy központi szerv. A kód mindenki számára hozzáférhető és futtatható. A blokklánc-orákulum pedig a titkos hozzávaló, hiszen ezek a rendszerek zártan működnek, a kihívás a hiteles és korrekt adat betöltése az okosszerződésekbe (blockchain oracle problem). A Delphi jósda az ókori Görögország egyik legfontosabb helyszínének számított, ahol uralkodók és egyszerű emberek fordulhattak tanácsért és útmutatásért az igazság görög istenéhez, Apollóhoz. Az orákulum szó eredeti jelentése is közvetítő. A jósdák egyfajta hídként szolgáltak a görög mitológiában is. Juels regényében a Delphi jósda modern analógiája a blokklánc orákulumok, információforrásként szolgálnak az okosszerződések számára, lehetővé téve számukra, hogy hitelesített adatok alapján hajtsanak végre tranzakciókat.

Juels karaktereiben többféle szubkultúrát látunk visszaköszönni. A főszereplőt anonimként ismerjük meg, akit technikai szakemberként érdekel a történelem is. Szabadidejében a technológiáról blogot ír ismeretterjesztő szándékkal. Mintegy fricskát mutatva az akadémiai köröknek, mondja: "ennek a Cornell professzornak a tanulmányait nem olvasom, hiszen előre megjósolható, miről fog írni". A történetbe bekapcsolódik többek között az amerikai filmekből ismert FBI-nyomozó karakter,

antik görög mitológiáért rajongó kutató, Z generációs kriptovaluta-natív és egy vezető befektetési bank menedzsere is. Ezek a karakterek széles spektrumát mutatják be azoknak, akik a blokklánc és a kriptovaluta világában (is) mozognak.

A fordulatos események mellett a technikai részletek is helyet kaptak a történetben, részletesen olvashatunk például egy új pénzügyi termékről, a „multi-block flash loan"-ról. A villámkölcsön (*flash loan*) decentralizált pénzügyi termék, a multi block flash loan ennek változata. A villámkölcsönök lényege, hogy a kölcsön felvétele és visszafizetése egyetlen blokkon belül történik, ami azt jelenti, hogy az egész folyamat pár másodpercet vehet igénybe a blokklánc sebességétől függően. A villámkölcsönöket gyakran használják különböző pénzügyi stratégiákhoz, mint például arbitrázs, anélkül, hogy a felhasználónak saját tőkét kellene bevonnia. Mivel a kölcsön és a visszafizetés egy tranzakcióban történik, a kölcsön csak akkor sikerül, ha a kölcsönösszeg teljes egészében visszafizetésre kerül a tranzakció végére. Ha a visszafizetés nem történik meg, a tranzakció visszavonásra kerül, mintha soha nem is történt volna meg. Ez minimalizálja a kölcsönt nyújtó fél kockázatát, de magas szintű technikai tudást és piaci ismereteket igényel a felhasználótól. A multi-block flash loan-ok több blokkon keresztül terjedő tranzakciókat tesznek lehetővé. Ez azt jelenti, hogy a felhasználó több időt kap a kölcsönzött összeg felhasználására és visszafizetésére, ami bonyolultabb pénzügyi műveletek, például összetettebb arbitrázs-stratégiák vagy más, időigényesebb tranzakciók végrehajtását teszi lehetővé. A multi-block flash loan-ok esetében a felhasználónak biztosítania kell a kölcsön és a hozzá kapcsolódó díjak visszafizetését több blokk alatt, ami nagyobb rugalmasságot és lehetőséget biztosít, de ezzel együtt a sikeres visszafizetés biztosításának kihívásait is magában hordozza.

A történet etikai dilemmákat is boncolgat, rávilágítva, hogy a blokklánc-technológia és mesterséges intelligencia kombinálása váratlan következményekkel járhat. A főhős, akinek hitében megkérdőjelezhetetlen az okosszerződések integritása, szembesül a dilemmával, amikor az FBI megkéri, hogy hackelje meg a blokklánc-orákulumot. Emellett felmerül az is, a nyílt forráskódú és nyilvánosan elérhető okosszerződések használata komoly tudást igényel, felvetve a kérdést, hogy vajon mindenki számára biztonságos-e a használatuk, vagy csak a jól képzett szakemberek kezében.

Az okosszerződés lényegét tekintve számítógépes kód, előnyük, hogy egyértelműek és egzakt „szerződéseket" érvényesíthetünk velük egymás között. A valóságban azonban emberi nyelven kommunikálunk, ami számtalanféle asszociációra ad teret. A nagy nyelvi modellek (LLM) viszont képesek lehetnek egyfajta felületként, fordítóként működni az emberek, intézmények és a blokklánc-rendszerek között. A könyv általános üzente az, hogy a technológia alapvetően semleges, jó és rossz célra egyaránt felhasználható. Anélkül, hogy lelepleznénk a Delphian „bűnszervezetet" a könyv másik üzenete, hogy először érdemes a mikrokörnyezetünkben vizsgálódni.

Ari Juels regénye fordulatokban gazdag, karakterei jól tükrözik az iparág szereplőinek gondolkodását és viselkedését. A blokklánc technológia alapvető működését és a technikai részleteket könnyen érthetően tárja elénk, ugyanakkor a téma iránt átlagosnál magasabb érdeklődést feltételez. Összegezve, a könyvet ajánlom minden a technológia és pénzügyek iránt érdeklődőnek, emlékeztetve arra, hogy egy sci-fi thriller regényt tartanak a kezükben.