

# **OTDK-dolgozat**

**2025**

**MILTON FRIEDMAN EGYETEM**



**Hármas könyvelési rendszer blokklánc technológia alkalmazásával**  
**Triple-entry accounting with blockchain technology**

**Györki Attila**

Konzulens: Dr. Szegediné Lengyel Piroska PhD

Főiskolai tanár

Dr. Honfi Vid Sebestyén PhD

Tanszékvezető, Informatika Tanszék

Kézirat lezárásának dátuma: 2025.01.09.

# TARTALOMJEGYZÉK

## Tartalom

|        |                                                                  |    |
|--------|------------------------------------------------------------------|----|
| 1.     | BEVEZETÉS .....                                                  | 1  |
| 2.     | A KÖNYVELÉS RÖVID TÖRTÉNETE .....                                | 3  |
| 2.1.   | A KEZDETEK .....                                                 | 3  |
| 2.2.   | A KÖNYVELÉS RENESZÁNSZA.....                                     | 3  |
| 3.     | A BLOKKLÁNC TECHNOLÓGIA .....                                    | 6  |
| 3.1.   | TÖRTÉNETE.....                                                   | 6  |
| 3.2.   | ALAPFOGALMAK.....                                                | 7  |
| 3.3.   | KAPCSOLATA A KÖNYVELÉS VILÁGÁVAL.....                            | 9  |
| 4.     | HÁRMAS KÖNYVELÉS.....                                            | 11 |
| 4.1.   | BLOKKLÁNC ALAPÚ KÖNYVELÉS .....                                  | 11 |
| 4.2.   | HAWK-MODELL.....                                                 | 14 |
| 5.     | BLOKKLÁNC ÉS KÖNYVELÉS.....                                      | 17 |
| 5.1.   | KÖVETKEZŐ GENERÁCIÓS APPLIKÁCIÓK .....                           | 17 |
| 5.2.   | KIHÍVÁSOK .....                                                  | 18 |
| 5.2.1. | Technológiai kihívások.....                                      | 18 |
| 5.2.2. | Adatbiztonság és adatvédelem.....                                | 19 |
| 5.2.3. | Interoperabilitás .....                                          | 21 |
| 5.2.4. | Implementációs költségek.....                                    | 22 |
| 6.     | HÁTTÉRINTERJÚ.....                                               | 24 |
| 6.1.   | INTERJÚ VIDÁKOVICS ATTILÁVAL- DLABS KFT - 2024.11.11.....        | 24 |
| 6.2.   | INTERJÚ SZABÓ PÉTERREL - SONEAS VEGYIPARI KFT. - 2024.11.14..... | 27 |
| 6.3.   | INTERJÚ ZSOLDOS LÁSZLÓVAL - OTP BANK - 2024.11.13 .....          | 29 |
| 7.     | KONKLÚZIÓ .....                                                  | 32 |
| 8.     | IRODALOMJEGYZÉK .....                                            | 35 |

## TÁBLÁZATJEGYZÉK

|                                                  |    |
|--------------------------------------------------|----|
| 1. táblázat Kettős könyvelés .....               | 11 |
| 2. táblázat "Vásárló-cég" könyvelése .....       | 11 |
| 3. táblázat "Eladó-cég" könyvelése .....         | 12 |
| 4. táblázat Blokklánc alapú főkönyv .....        | 13 |
| 5. táblázat Könyvek egyezősége.....              | 14 |
| 6. táblázat Eltérő főkönyvek család esetén ..... | 14 |

## ÁBRAJEGYZÉK

|                                        |    |
|----------------------------------------|----|
| 1. ábra Hawk-modell: aukciós séma..... | 16 |
|----------------------------------------|----|

## 1. BEVEZETÉS

A dolgozatban bemutatott blokklánc technológiára épülő könyvelési rendszer alapjaiban rendezheti át nem csak a könyvelői, de a könyvvizsgálói feladatokat is. A technológia megfelelő implementációjával az üzleti bizalom nőne, miközben rengeteg humán erőforrás szabadulna fel, és azokat hasznosabban lehetne a rendszerbe visszaforgatni. Ezenfelül a blokklánc használatával az automatizációhoz is közelebb kerülhet a számviteli szakma.

Az implementáció egyik legfőbb célja, hogy az adatok (tranzakció adatai) titkosítottak legyenek, de azoknak pontossága és megbízhatósága mégis ellenőrizhető maradjon harmadik fél (auditor) számára (Hawk-modell).

Dolgozatomban a könyvelés történetének rövid összefoglalása és a blokklánc technológia alapfogalmainak ismertetése után bemutatom Ian Grigg által 2005-ben megfogalmazott (majd 2024-ben újradolgozott) blokklánc segítségével történő könyvelés alapjait és a tranzakciók titkosítására használt Hawk-modellt rávilágítva arra, hogy mekkora potenciál rejlik a blokklánc pénzügyi és gazdasági felhasználásában. Fontos kiemelni a felmerülő kihívásokat (GDPR, átképzés, implementálási költségek), és az azokra irányuló lehetséges megoldási javaslatokat.

**Hipotézis:** A blokklánc technológia számviteli területen való felhasználásával a jelenlegi kettős könyvviteli rendszert kiegészítheti a „hármass könyvelés” elve, amely egy hitelesítő blokklánc alapú főkönyv bevezetésével megbízhatóbbá, átláthatóbbá és automatizálhatóbbá teheti a könyvelés menetét.

## MÓDSZERTAN

*A téma feldolgozásához primer kutatási módszertan keretében egy, a blokkláncsal foglalkozó magyar IT vállalkozás cégvezetőjével (DLabs Kft.) készített interjúanyagból próbálom a technológia jelenlegi állását és határait felmérni, a magyar bankszektorban készített interjúban (OTP Bank) körül járni a vállalati rugalmasságot és egy számviteli szakember segítségével (SONEAS Vegyipari Kft.) megismerni a számviteli szakma szempontjait.*

*Szekunder módszertannal a blokklánc könyviteli alkalmazásának eddig kutatott területeit mutatom be, illetve az alapvető fogalmakat ismertetem. A magyar szakirodalom szűkössége miatt dolgozatom túlnyomóan nemzetközi szakirodalomra épült, figyelembe véve azok relevanciáját és azt, hogy a technológia fejlődésének gyorsulása miatt friss kutatások és elemzések adnak valós képet a jelenlegi állapotokról.*

## 2. A KÖNYVELÉS RÖVID TÖRTÉNETE

### 2.1. A KEZDETEK

A számvitel olyan régi, mint a kereskedelem, hiszen mióta javak – vagy pénzeszközök – cserélik egymást, a gazdasági élet szervezéséhez és nyomon követéséhez elengedhetetlen feltétel volt, hogy ezt rögzítsék. Mondhatni a számvitel nem más, mint társadalmunk töretlen kísérlete arra, hogy nyomon kövessük a pénzügyi eseményeket. Így talán nem meglepő, hogy az első fellelhető könyvelési leletek több, mint 7000 évesek, az ősi Mezopotámiából származnak (Robson, 1992).

A könyvelés fejlődése főként templomokban és nagyobb gazdasági központokban indult meg, ahol árukészletet, munkaerőt és nyersanyagokat kellett nyomon követnie, és segítette a kereskedőket abban, hogy a különböző gazdasági folyamatokat nagyobb volumenben, ellenőrzés mentén kezeljék. Ez a könyvelés, még merőben eltér a napjainkban ismert és elterjedt kettős könyveléstől, hiszen úgymond „egyes” könyvelésről beszélünk, ahol a bevételt és kiadást először fába vésett rovásokkal, majd később ékírással agyagtáblákon vezették.

Beláthatjuk, hogy egy ilyen módon vezetett „főkönyv” hitelessége erősen megkérdőjelezhető, a könyv könnyedén másítható, és nincs semmilyen garancia arra, hogy a rögzített adatok valósak. Bár a könyvelési módszer hagy némi kivetnivalót maga után, Robson szerint jelentős hatással bírt az írás és számolás fejlődésére, valamint a konkrét számolásról az absztrakt számolásra való áttérésre.<sup>1</sup>

### 2.2. A KÖNYVELÉS RENESZÁNSZA

*„A bizalom, a jó hírű üzletemberekbe vetett hit az, ami hatékonyá teszi a piacot.”*

*Luca Pacioli*

A fenti idézet tökéletesen leírja, mi az, ami hiányzott a reneszánsz korig a könyvelésből. A Bizalom.

Előzőleg említésre került, hogy az „egyes könyvelés” legfőbb hibája, hogy ellenőrizhetetlen, az adatok könnyedén másíthatóak, és külső szemlélőnek meg kell bíznia az agyagtáblában, abban, hogy az ott látható adatok valósak.

---

<sup>1</sup> Konkrét számolásnak hívjuk, a valós tárgyakhoz való számrendelést, például kövekkel, abakusszal, míg az absztrakt számolás egy fejlettebb gondolkodásmód, ahol maga a szám önállóan, mint mérce jelenjen meg, hozzá rendelt valós tárgy nélkül, így adott dolgokat „összehasonlíthatóvá” tesz.

A világ felfedezésével a kereskedelem a reneszánszban felvirágzott, és ennek köszönhetően a Vatikán és az olasz banki városok – Genova, Velence, Firenze – aranykorukat élték. A bankok már rögzítették a tranzakciókat, kölcsönöket nyújtottak. Ezeknek a folyamatoknak a lekövetése megkövetelte, sőt magában hordozta a számvitel fejlődését.

Bár Luca Paciolit nevezzük a „könyvelés atyjának” és legtöbbször hozzákötik a kettős könyvelés rendszerét, a kettős könyvelés már a 14. században megjelent a Medici családnak hála. Bár a módszer korábban is ismert volt<sup>2</sup>, Giovanni de’ Medici – saját maga alapított bankjában – vezette be elsőként napi felhasználásban a kettős könyvelést és emellett rengeteg olyan dolgot, amik a mai globális bankok működésében is megtalálhatóak: egységes üzemi szabályok, központi irányítás, leányvállalatok (Fazzini, Fici, Montrone, & Terzani, 2016).

Az igazi áttörést mégis Luca Pacioli hozta el a „Summa de Arithmetica, Geometria, Proportioni et Proportionalitá”<sup>3</sup> című művében, ami többek közt annak is volt köszönhető, hogy azt nem latinul, hanem anyanyelven publikálta, illetve még da Vinci támogatását is élvezte. Ebben a művében ismertette nem csak a kettős könyvelés módszertanát, de az arab számjegyeket is.

A könyvelésben jól ismert „tartozik” és „követel” szavak is itt jelentek meg először: „credre” (megbízni) – „debere” (tartozni), aminek a hasonlóságát főképp az angol szaknyelvben lelhetjük fel: debit (tartozik) és credit (követel). Módszertanában lefekteti a ma is ismert könyvelés alapjait a főkönyv, napló és jegyzőkönyv ismertetésével.

A megnövekedett Földközi-tengeri kereskedelem, az olasz városállamok közti kereskedelem és a banki hitelezések elterjedése megkövetelte, hogy a pénzmozgásokat megbízható módon vezessék, a hiba (és csalás) lehetőségét minimalizálják, amire az eddig ismert könyvelési technikák nem voltak alkalmasak.

---

<sup>2</sup> A legrégebbi ismert feljegyzés egy 1340-es genovai lajstromban található (Ototea, 1974)

<sup>3</sup> „Mindent az aritmetikáról, geometriáról és arányokról”

A különböző gazdasági szereplők (bankok, államok, céhek) számára standardizálható, egységes keretrendszer biztosította, hogy szakmabélieknek a könyvek mindig „egyszerűen” értelmezhetőek, a könyvvezetések logikája egységesíthető. Nem véletlen, hogy – kisebb-nagyobb változtatásokkal – a kettős könyvelés azóta is világszerte uralkodó főkönyvelési módszertan. Természetesen, mint minden rendszernek ennek is meg vannak a hátrányai, hiszen a könyveket csak szakértők tudják értelmezni, ezért azoknak hitelességét rendszeres könyvvizsgálatokkal kell biztosítani, a könyvek vezetése a mai napig emberi munkaerőt igényel, és csak az nem hibázik, aki nem dolgozik. Vagy, aki algoritmus.

### 3. A BLOKKLÁNC TECHNOLÓGIA

*„A magánélet szükséges az elektronikus kor nyílt társadalmához. ... Nem várhatjuk el, hogy a kormányok, vállalatok vagy más nagy, névtelen szervezetek önzetlenségükből adjanak nekünk magánéletet. Előnyünkre válik, ha mindent titkosítunk.”*

*Eric Hughes, 1993*

#### 3.1. TÖRTÉNETE

A fejezethez érve, feltehetnénk a kérdést, mi is az a blokklánc, de a Cypherpunk Manifestóból idézve, megelőzve a „mi” kérdésre való választ, megadtam a „miért” -re (Hughes, 1993). De elég lefordítanunk David Chaum 1982-es disszertációjának címét (amiben már blokklánc-jelleggel találkozhattunk), hogy megértsük a miértet: „Computer System Established, Maintained and Trusted by Mutually Suspicious Groups”. „Kölcsönösen gyanakvó csoportok”.

A világ előrehaladásával, a kapitalizmus kiforrásával és a központosított rendszerek globalizációjával egyre erősebb igény volt arra, hogy az egyén újból saját maga rendelkezessen az adataival. Ha a dolgozunk, a munkáltatónk megbíz egy harmadik felet (bank), hogy utalja el a fizetésünket a számlánkra, majd mi megbízzuk a bankot, hogy tárolja azt, és igény esetén bocsássa rendelkezésre. Minden egyes tranzakcióhoz szükségünk van egy harmadik félre, és annak a kiépített infrastruktúrájára, amin keresztül minden adat áthalad.

A fent említett disszertációban még nem a ma ismert blokkláncról beszéltünk, de a gondolat már ott volt. A ma ismert formájának elnyeréséig folyamatos evolúción haladt végig attól függően, hogy ki mit tartott fontosnak: a cypherpunk mozgalom a „titokhoz való jogot”, volt, aki a digitális aláírásokat vagy éppenséggel a smart contractokat.

A blokklánc, mint fogalom első megjelenését 1991-re datáljuk Stuart Haber és W.Scott Stornetta nevéhez kötve. Az ő elsődleges céljuk az volt, hogy különböző dokumentumok időbélyeggel való ellátását követően biztosíthassák annak integritását, megmásíthatatlanságát. Az évek során több elmélet (és gyakorlat) is született a blokklánc felhasználásáról, de az igazi áttörést 2008-ban Satoshi Nakamoto<sup>4</sup> hozta el a „A Peer to Peer Electronic Cash System” című publikációjával, amiben az előző évek kutatásait (Proof of Work, Merkle-fa)

---

<sup>4</sup> Álnév, a mai napig nem ismert, hogy ki áll a „Satoshi” név mögött.

finomította, és ennek köszönhetően 2009-ben megszületett a Bitcoin. A mai napig az emberek többsége, ha a blokklánc szót meghallja, kizárólag kriptovalutákra gondol, annak ellenére, hogy a már 2014 óta a fejlesztések elvonatkoztattak a blokklánc valuta alapú felhasználásától, és ezt hívták „Blokklánc 2.0” -nak.

### 3.2. ALAPFOGALMAK

**Blokklánc:** Ha számviteli metaforát szeretnénk használni, akkor mondhatjuk, hogy egy decentralizált digitális főkönyv, amely blokkjaiban időrendi sorrendben adatokat tárolunk, ezek egymásra épülnek és a blokkok közti erős kriptográfiai kapcsolatnak köszönhetően az adatok utólag nem módosíthatóak.

Decentralizáltság alatt azt értjük, hogy nincs egy központi adatbázis, ahol ez nyilván van tartva, hanem a főkönyv másolata a hálózat minden résztvevőjénél ott van. Példának okáért, a mindenki által ismert Bitcoin esetében ez nem más, mint a tranzakciók adatainak hasshé (lenyomattá) formálása egy SHA-256 nevezetű algoritmussal. Nem tudunk Bitcoint lopni, hisz a „főkönyv” ott van mindenkinél, és több tíz-, vagy akár százezer főkönyvet kéne átírni ahhoz, hogy a rendszert átverjük.

**Hash:** A hash egy kriptográfiai módszer, amellyel tetszőleges nagyságú bemenetből egy fix hosszúságú, egyedi karaktersorozatot (lenyomat) generálhatunk. A módszer determinált, azaz ugyanaz a bemeneti adat, mindig, pontosan ugyanazt a hash értéket eredményezi. A legkisebb változtatás (kisbetű/nagybetű eltérés is!) jelentősen változtatja a hash értékét. A hashelés visszafordíthatatlan, így a karaktersorozatból az eredeti bemeneti érték (vagy adat) nem visszafejthető. További előnye, hogy ütközésálló, tehát annak az esélye, hogy két különböző adatból véletlenszerűen pontosan ugyanaz a karaktersorozat jöjjön létre, minimális (az általánosan használt, SHA-256-os hash függvény esetén, ahhoz, hogy 50%-os eséllyel találjunk két különböző bemenetet ugyanazzal a hash-értékkal,  $2^{128}$  különböző bemenetet kellene kipróbálnunk). A dolgozat témáját illetően a hash legfontosabb tulajdonságai és felhasználási területei:

- **Adatbiztonság:** A hash-függvény determinált mivoltának köszönhetően a tranzakciók részletei biztonságosan tárolhatóak.
- **Hitelesítés:** a determinisztikus jellege segít abban, hogy például egy tranzakció utólag ne legyen megváltoztatható (hisz a bemenet legkisebb változtatása is jelentősen változtatja a hash-értéket)

- **Blokklánc:** A hash az egyik alapja a blokklánculat kialakulásának, mivel minden blokk tartalmazza az őt megelőző blokk hash-értékét, így egy „múltbéli” blokk megváltoztatása (pl. csalás) minden azt követő blokkra kihatással lenne.
- **Összehasonlítás:** mivel a tranzakciókat hashelt formában tárolhatjuk két különböző helyen is, könnyedén összehasonlítható, hogy két főkönyvben pontosan ugyanaz a tranzakció szerepel-e (ha eltér a hash, valamelyik érték hibás).

**Smart Contract:** azaz okos szerződés, egy olyan számítógépes protokoll, amely lehetővé teszi szerződések automatikus végrehajtását a blokklánc hálózaton, előre meghatározott feltételek teljesülése esetén.

A szerződések közvetítő nélkül, programozott módon valósulnak meg, így a szerződések a szerződő felek számára biztonságosabb és gyorsabb megoldást kínálnak. Például, „Vásárló-cég” okos szerződésbe foglalja „Eladó-céggel”, hogy az „Áru” átvételét követően fizeti ki a 100\$-os vételárat. A 100\$ „letétbe” kerül az okos szerződésnél, aminek a teljesülési feltétele, az áruátvételi nyilatkozat digitális aláírása. Amint az algoritmus meggyőződik róla, hogy az átvétel megtörtént, a 100\$-t automatikusan továbbítja „Eladó-cégnek”.

További kitétel lehet például, hogy amennyiben az „Áru” adott dátumig nem érkezik meg, a letétet szabadítsa fel a „Vásárló-cég” részére. Így mindkét fél bizalommal lehet a másik felé: „Eladó-cég” tudhatja, hogy „Vásárló-cég” -nek van erre tőkéje, és „Vásárló-cég” is biztos lehet benne, hogy nem teljesülő szállítást esetén, nem kell rohangálni a pénz után. Ilyen, és hasonló implementációkkal az üzleti bizalom nőhet, hisz a tranzakciók megtörténe algoritmusvezérelté válik.

**Digitális aláírás:** egy olyan kriptográfiai módszer, ami igazolja egy digitális dokumentum, vagy adat hitelességét, integritását és eredetiségét. A mai világban elterjedt mód arra, hogy ezzel hitelesítsük, hogy az adott dokumentumot, az adott személy hozta létre, és a létrehozás óta senki nem módosított bele. A könyvelés világában számunkra fontos tulajdonságai:

- **Hitelesség:** a résztvevő felek az aláírásukkal hitelesítik, hogy az adott tranzakció ténylegesen megtörtént
- **Integritás:** az aláírás biztosítja, hogy a már rögzített adatok nincsenek manipulálva, utólag módosítva.

- **Átláthatóság:** a hitelesség és integritás együttesével az auditálás során könnyebb megbizonyosodni egy adott tranzakció valóság tartalmáról.

**Privát kulcs és nyilvános kulcs:** a digitális aláírások technikai háttere. Létezik egy privát kulcs, amit csak az „aláíró” ismer, és egy ehhez a kulcshoz tartozó nyilvános kulcs, ami mindenki számára elérhető; ezzel a nyilvános kulccsal győződhetünk meg róla, hogy az aláírás hiteles. Ezeket a kulcsokat aszimmetrikus titkosítási algoritmussal hozzák létre (RSA vagy ECC általában), a privát kulcs egy 2048 vagy 4096 bit hosszú kód, majd ebből hoznak létre egy ehhez „passzoló” nyilvános kulcsot. Ha a kulcspár passzol, az aláírás hiteles.

### 3.3. KAPCSOLATA A KÖNYVELÉS VILÁGÁVAL

A technológia alapfogalmainak megismerése után beláthatjuk, hogy miért foglalkoznak egyre aktívabban a blokklánc helyének megtalálásával a könyvelés és számvitel világában is. Titkosítás, hamisíthatatlanság, automatizáció és átláthatóság.

Az ACFE (Association of Certified Fraud Examiners) jelentése szerint, 2024-ben 3,1 milliárd dollár kárt okoztak a foglalkozási körben elkövetett csalások, aminek esetszámaiból csupán csak 5%-ot tesz ki a pénzügyi kimutatásokat érintő csalás, de a medián veszteség, amit okoz, a maradék 95% eset mediánjának kétszerese (Association of Certified Fraud Examiners, 2024). Az átláthatóság érdekében természetesen a kettős könyvvitel is fejlődött Pacioli óta (IFRS szabványok, számviteli törvények stb.), ennek ellenére a bizalomhiányt a jelenlegi rendszerben nem lehet teljes mértékben kiküszöbölni.

A Bitcoin 15 éves pályafutása és stabil működése az, ami rámutatott arra, hogy ideje újra gondolni a jelenlegi rendszert, és megtalálni a blokklánc felhasználási területét a számvitelben is. Jelenleg – 2024 október – több mint 700 ezer tranzakció történik naponta a Bitcoin hálózaton (Bitcoin Transactions per Day, 2024), amik mindegyike algoritmus és a hálózat konszenzusmechanikája által hitelesített tranzakció. Nincs felügyeleti szerv, aki könyveli a Bitcoinok tulajdonosváltását, nincs egy adatbázis, ami túlterhelődhetne a túl nagy forgalom alatt. A tranzakciók hitelességét nem emberek, hanem algoritmusok végzik automatikusan és az azokban tárolt adatok utólag már nem változtathatóak.

Ha végig gondoljuk, hogy eddig milyen tulajdonságairól beszéltünk a blokkláncnak, gyorsan rájövünk, hogy pontosan ilyen tulajdonságokat szeretnénk egy főkönyvnek: egy megmásíthatatlan, decentralizált, de mégis hiteles főkönyvet.

A blokklánc alkalmazása esetén út nyílna az automatizáció fokozására is, a valós idejű tranzakció kezelés révén a pénzügyi állapotokat folyamatosan nyomon követhetné a vállalat, ami alapjaiban változtatná meg a jelenlegi éves-, negyedéves beszámoló ciklusokat, vagy akár a cash-flow számításokat. Ezeknek a változásoknak hála, a jelentések naprakészek lennének, ami növelné a piaci szereplők (befektetők) bizalmát, és alaposabb stratégiai döntéseknek alapozna meg.

A valósidejűség másik hatása a könyvelők munkakörének gyökeres megváltozása, hiszen az automatizáció felgyorsítaná az eddig hosszadalmas és időigényes folyamatokat, így a könyvelők több energiát tudnának befektetni a gazdasági események elemzésébe, gazdasági folyamatok lekövetésébe.

## 4. HÁRMAS KÖNYVELÉS

### 4.1. BLOKKLÁNC ALAPÚ KÖNYVELÉS

Ian Grigg „Triple Entry Accounting” írásában felvetette (Grigg, 2024)<sup>5</sup>, hogy a hagyományos kettős könyvelés és az akkor már megjelent, digitális nyugtákat nem egymás mellett, hanem egymással kell használni, így létrehozva a hármas könyvelés alap elképzelését.<sup>6</sup> A kettős könyvelés során minden gazdasági esemény két számlán és kétféle rendszerben (idő-soros elszámolás és számlasoros elszámolás) kerül rögzítésre.

„Vásárló-cég” rendszeresen vásárol üzemanyagot az „Eladó-cég” saját üzemanyag készletéből, amit készpénzzel fizet ki. A tranzakciók a kettős könyvelés rendszere szerint megjelennek a cégek főkönyvi számláin (1.táblázat) és a cégek könyvelési naplójában (2.táblázat, 3.táblázat).

| "Vásárló-cég" |         |             |           | "Eladó-cég"  |           |             |         |           |         |               |           |
|---------------|---------|-------------|-----------|--------------|-----------|-------------|---------|-----------|---------|---------------|-----------|
| 222 Üzemanyag |         | 381 Pénztár |           | 91 Árbevétel |           | 381 Pénztár |         | 814 ELÁBÉ |         | 222 Üzemanyag |           |
| Tartozik      | Követel | Tartozik    | Követel   | Tartozik     | Követel   | Tartozik    | Követel | Tartozik  | Követel | Tartozik      | Követel   |
| \$ 100,00     |         |             | \$ 100,00 |              | \$ 100,00 | \$ 100,00   |         | \$ 50,00  |         |               | \$ 50,00  |
| \$ 150,00     |         |             | \$ 150,00 |              | \$ 150,00 | \$ 150,00   |         | \$ 75,00  |         |               | \$ 75,00  |
| \$ 200,00     |         |             | \$ 200,00 |              | \$ 200,00 | \$ 200,00   |         | \$ 100,00 |         |               | \$ 100,00 |

1. táblázat Kettős könyvelés  
(Forrás: saját szerkesztés)

| "Vásárló-cég" |                    |          |         |           |
|---------------|--------------------|----------|---------|-----------|
| Dátum         | Gazdasági esemény  | Számla   |         | Összeg    |
|               |                    | Tartozik | Követel |           |
| 2024.10.01    | Üzemanyag vásárlás | 222      | 381     | \$ 100,00 |
| 2024.10.06    | Üzemanyag vásárlás | 222      | 381     | \$ 150,00 |
| 2024.10.11    | Üzemanyag vásárlás | 222      | 381     | \$ 200,00 |

2. táblázat "Vásárló-cég" könyvelése  
(Forrás: saját szerkesztés)

<sup>5</sup> Az eredeti verzió 2005-ben jelent meg, viszont 2024-ben a „Journal of Risk and Financial Management”-ben egy aktualizált verziója került publikálásra.

<sup>6</sup> Yuji Iriji már 1989-ben megfogalmazta a hármas könyvelést, de ő akkor még nem blokklánc alapon képzelte el, hanem úgynevezett „momentum-könyvelés”-ként, ami nem csak statikus mérlegekre (eszközök, források) fókuszál, hanem a változások sebességét és gyorsulását is figyelembe veszi (Yuji, 1989).

| "Eladó-cég" |                                    |          |         |           |
|-------------|------------------------------------|----------|---------|-----------|
| Dátum       | Gazdasági esemény                  | Számle   |         | Összeg    |
|             |                                    | Tartozik | Követel |           |
| 2024.10.01  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 100,00 |
| 2024.10.01  | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 50,00  |
| 2024.10.06  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 150,00 |
| 2024.10.06  | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 75,00  |
| 2024.10.11  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 200,00 |
| 2024.10.11  | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 100,00 |

3. táblázat "Eladó-cég" könyvelése  
(Forrás: saját szerkesztés)

Tételezzük fel, hogy az üzemanyag árak miatt az üzemanyag-költségekből a cégek állami visszatérítést igényelhetnek, ezért „Vásárló-cég” egy idő után az üzemanyag költségeket meghamisítaná: egy 100\$-os vásárlást, 101\$-on könyvelne el, így jogtalan előnyhöz juttatva magát a visszatérítés során. Lévén, hogy rendszeres vásárlásról van szó, rengeteg naplóbejegyzés jönne létre, aminek köszönhetően csak egy részletes könyvvizsgálat során derülhetne ki a hamisítás.

Ellenben, a hármas könyvelés során, minden egyes tranzakció a digitális bizonylatokkal jönne létre smart contractok segítségével: a tranzakció könyvelésre kerülne hagyományosan a könyvviteli naplóban idősorosan és a főkönyvi számlákon, azzal a változással, hogy a könyvviteli naplóban a tranzakciókhoz a hash is hozzátartozna (5.táblázat). Ezenfelül mint harmadik könyv, a tranzakció megjelenne a közös blokkláncon is, mindkét félre vonatkozó adatokkal (4.táblázat). Ez a blokklánc lesz az, ami egy megmásíthatatlan ellenőrzési pontot ad a rendszernek, hiszen ennek a szerkesztése nem lehetséges, a blokkok kizárólag a smart-contractok (megvalósult tranzakciók) által tudnak létrejönni.

| Blokklánc  |                                                                  |                                       |               |         |             |         |           |
|------------|------------------------------------------------------------------|---------------------------------------|---------------|---------|-------------|---------|-----------|
| 1.blokk    |                                                                  |                                       |               |         |             |         |           |
| Előző hash |                                                                  |                                       |               |         |             |         |           |
| Időbélyeg  | 2024.10.01 16:34                                                 |                                       |               |         |             |         |           |
| Adat       | Dátum                                                            | Gazdasági esemény                     | "Vásárló-cég" |         | "Eladó-cég" |         | Összeg    |
|            |                                                                  |                                       | Tartozik      | Követel | Tartozik    | Követel |           |
|            | 2024.10.01                                                       | Üzemanyag értékesítés                 | 222           | 381     | 381         | 91      | \$ 100,00 |
|            | 2024.10.01                                                       | Üzemanyag értékesítés<br>(Ráfordítás) | -             | -       | 814         | 222     | \$ 50,00  |
| Hash       | 941bac20299206efe247f67c0db5b342ac84d890f041590d9502bc29b1c04f66 |                                       |               |         |             |         |           |
| 2.blokk    |                                                                  |                                       |               |         |             |         |           |
| Előző hash | 941bac20299206efe247f67c0db5b342ac84d890f041590d9502bc29b1c04f66 |                                       |               |         |             |         |           |
| Időbélyeg  | 2024.10.05 10:21                                                 |                                       |               |         |             |         |           |
| Adat       | Dátum                                                            | Gazdasági esemény                     | "Vásárló-cég" |         | "Eladó-cég" |         | Összeg    |
|            |                                                                  |                                       | Tartozik      | Követel | Tartozik    | Követel |           |
|            | 2024.10.05                                                       | Üzemanyag értékesítés                 | 222           | 381     | 381         | 91      | \$ 150,00 |
|            | 2024.10.05                                                       | Üzemanyag értékesítés<br>(Ráfordítás) | -             | -       | 814         | 222     | \$ 75,00  |
| Hash       | 4598bc58e830395f41a102b2c02adfe15128aabf4b4e8ca59bad624f436cbf19 |                                       |               |         |             |         |           |
| 3.blokk    |                                                                  |                                       |               |         |             |         |           |
| Előző hash | 4598bc58e830395f41a102b2c02adfe15128aabf4b4e8ca59bad624f436cbf19 |                                       |               |         |             |         |           |
| Időbélyeg  | 2024.10.11 13:12                                                 |                                       |               |         |             |         |           |
| Adat       | Dátum                                                            | Gazdasági esemény                     | "Vásárló-cég" |         | "Eladó-cég" |         | Összeg    |
|            |                                                                  |                                       | Tartozik      | Követel | Tartozik    | Követel |           |
|            | 2024.10.11                                                       | Üzemanyag értékesítés                 | 222           | 381     | 381         | 91      | \$ 200,00 |
|            | 2024.10.11                                                       | Üzemanyag értékesítés<br>(Ráfordítás) | -             | -       | 814         | 222     | \$ 100,00 |
| Hash       | e6192a3aaf766fa9b27a0b7d1ad86aa3cad2c67ce3c3838a90b610330f9fa352 |                                       |               |         |             |         |           |

4. táblázat Blokklánc alapú főkönyv  
(Forrás: saját szerkesztés)

Az adott blokk tartalmazza mindkét főkönyv számára az információt, a blokk létrejöttének időpontját, illetve az előző hashből, időbélyegből és adatmezőből (tranzakció részletei) képzett hasht. Mivel a következő blokk az előző hash-karaktersorozatával kezdődik, így az előző blokkok érinthetetlenek, a blokklánc, mint egy harmadik, felek közti közös főkönyv hitelesít minden tranzakciót.

A példában három esemény került rögzítésre, de amennyiben két fél között egy évben akár 1000 tranzakció is létrejön, a tranzakciók egyezőségéről, és hitelességéről másodpercek alatt meggyőződhetünk, hisz kizárólag az utolsó hash egyezőségét (napló és blokklánc közt) kell vizsgálni. Ha az utolsó hash stimmel, a tranzakciók hitelesek. Amennyiben a két hash eltér egymástól, úgy az audit során meg kell keresni az utolsó egyező hasht. Beláthatjuk, mivel az összehasonlítást leegyszerűsítettük egy karaktersorozat összehasonlítására, így ezt könnyedén végezheti egy algoritmus is. Amennyiben akármelyik fél félrekönyvel a tranzakciók során, akár véletlenül, akár szándékosan, a végső hash el fog térni.

| "Vásárló-cég" |                    |          |         |           | "Eladó-cég" |                                    |          |         |           |
|---------------|--------------------|----------|---------|-----------|-------------|------------------------------------|----------|---------|-----------|
| Dátum         | Gazdasági esemény  | Számla   |         | Összeg    | Dátum       | Gazdasági esemény                  | Számla   |         | Összeg    |
|               |                    | Tartozik | Követel |           |             |                                    | Tartozik | Követel |           |
| 2024.10.01    | Üzemanyag vásárlás | 222      | 381     | \$ 100,00 | 2024.10.01  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 100,00 |
|               |                    |          |         |           |             | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 50,00  |
| 2024.10.06    | Üzemanyag vásárlás | 222      | 381     | \$ 150,00 | 2024.10.06  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 150,00 |
|               |                    |          |         |           |             | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 75,00  |
| 2024.10.11    | Üzemanyag vásárlás | 222      | 381     | \$ 200,00 | 2024.10.11  | Üzemanyag értékesítés (Bevétel)    | 381      | 91      | \$ 200,00 |
|               |                    |          |         |           |             | Üzemanyag értékesítés (Ráfordítás) | 814      | 222     | \$ 100,00 |

5. táblázat Könyvek egyezősége  
(Forrás: saját szerkesztés)

A hash véletlenszerűségének, és érzékenységének bemutatásául, az utolsó tranzakcióban 200\$ helyett, 201\$-t könyvelt el a „Vásárló-cég”, míg az „Eladó-cég” becsületesen az eredeti összeget (200\$) könyvelte: 1 dollár különbség, és mégis a hashek teljesen eltérnek (6.táblázat).

| "Vásárló-cég"                                                    |                                                                  |                                                                  |  |  | "Eladó-cég"                                                      |                                                                  |                                                                  |  |  |
|------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------|--|--|------------------------------------------------------------------|------------------------------------------------------------------|------------------------------------------------------------------|--|--|
| 941bac20299206efe247f67c0db5b342ac84d890f041590d9502bc29b1c04f66 | 4598bc58e830395f41a102b2c02adfe15128aabf4b4e8ca59bad624f436cbf19 | 9345634cf4bb49f962169d41dd332a145827b4d7160ba39eebf59b1fef33e4ac |  |  | 941bac20299206efe247f67c0db5b342ac84d890f041590d9502bc29b1c04f66 | 4598bc58e830395f41a102b2c02adfe15128aabf4b4e8ca59bad624f436cbf19 | e6192a3aaf766fa9b27a0b7d1ad86aa3cad2c67ce3c3838a90b610330f9fa352 |  |  |

6. táblázat Eltérő főkönyvek család esetén  
(Forrás: saját szerkesztés)

Továbbá láthatjuk azt is, hogy ezzel a módszerrel, a külső könyvvizsgáló cégek hitelesen és gyorsabban tudják ellenőrizni a tranzakciókat úgy, hogy közben a rálátásukat a cégünk tranzakcióra megvontuk egészen addig a pontig, amíg egyezőség van. Emberi beavatkozásra, elemzésre és kiértékelésre csak abban az esetben van szükség, ha eltérést tapasztal az algoritmus és abban az esetben is kizárólag az első hibás bejegyzéstől kezdődően.

## 4.2. HAWK-MODELL

A korábban említett, blokklánc alapú okos szerződések alapvető problémája a nyilvánosság. Mivel egy „nyilvános főkönyvről” beszélünk, a blokklánc minden résztvevője egy másolatot tárol az összes tranzakcióról. Bitcoinnál nyilvánosan elérhető, hogy melyik feladó, melyik címzettnek mekkora összeget küldött. Természetesen a feladó nevénél egy alfanumerikus cím (publikus kulcs) fog megjelenni, de amennyiben kötni tudjuk valakihez a publikus kulcsot, úgy onnantól kezdve a tranzakcióit is nyomon követhetjük.

A Hawk-modell célja, hogy egy olyan kriptográfiai keretrendszert hozzon létre, amely lehetővé teszi privát, titkosított okos szerződések létrehozását úgy, hogy az adatintegritást, és megbízhatóságot megőrzi: így a tranzakciók titkosíthatóak, és az okos szerződések nem fednek fel semmilyen érzékeny adatot (Zéman, 2021).

A modellben a résztvevőket két részre osztják: „megbízott félre” és „blokkláncra”. Az eddigiektől eltérő szereplő, a megbízott fél: ő az, aki végre hajtja a szerződés specifikus elemeit, felel az adatok privát kezeléséért, miközben a blokklánc továbbra is az adatintegritásért kezkeskedik.

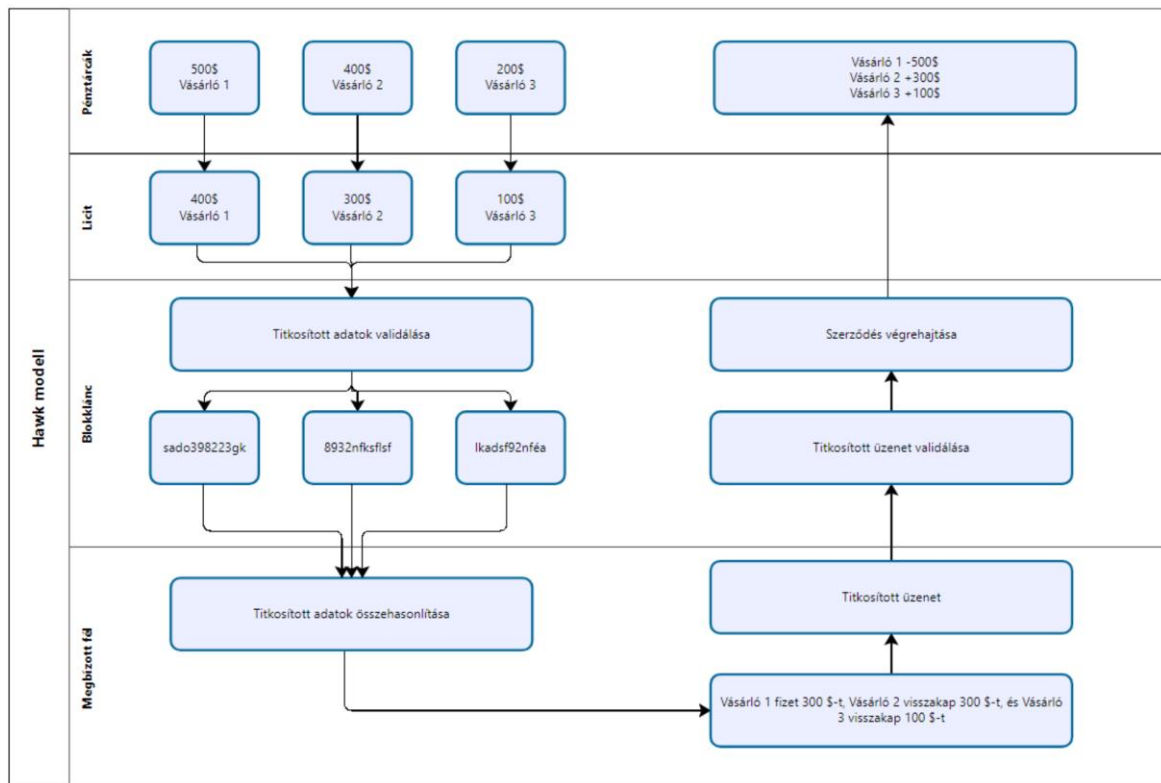
A modell legnagyobb innovációja a „zero-knowledge proof”: anélkül meg lehet bizonyosodni egy tranzakció hitelességéről, hogy ismernénk a részleteit. Legegyszerűbb példa rá, ha a születési dátumom egy megadott kriptográfiai módszerrel tárolom, anélkül igazolhatom, hogy elmúltam 18 éves, hogy a pontos életkoromat nem kell megadnom.

A homomorfikus titkosítás<sup>7</sup> segítségével, egy betanított algoritmus úgy tud műveletet végezni adatokkal (mai dátum – születési dátum > 18?), hogy azok titkosítva maradnak mindvégig: az algoritmus eldönti, hogy az így kapott dátum 18 évnél régebbi vagy sem, majd a végfelhasználó (eladó) számára zöld vagy piros jelzéssel tudtára adja, kiszolgálhat-e vagy sem. Az érzékeny adat (születési dátum) felfedése nélkül bizonyíthatjuk a feltétel beteljesülését. Egy másik szemléltető példa a „Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts”-ban is levezetett aukciós szimuláció (Kosba, Miller, Shi, Wen, & Papamanthou, 2016): az aukció során, a licitálók titkosan tesznek ajánlatot, ahol a legmagasabb árat licitáló nyer, de csak a második legmagasabb licittel megegyező árat kell fizetnie.

A blokklánc a licitek összegét, vagy tulajdonosát nem ismerheti, de azt validálni tudja, hogy a licit valós, a tulajdonosának van ennyi pénze. Ezt követően lép be a képbe a „megbízott fél”, egy privát protokoll, ami kiszámolja, hogy ki nyert (legmagasabb licit tulajdonosa) és mennyit kell fizetnie (második legmagasabb licit). Ezek a számítások a blokkláncon kívül történnek, így azok nem hozzáférhetőek, majd végül a blokkláncra visszakerül a számított eredmény, aminek hitelességét a blokklánc újfent ellenőrzi. Ezt követően a kifizetéseket végrehajtják (1.ábra)

---

<sup>7</sup> A homomorf titkosítás (RSA, Paillier, ElGamal) olyan titkosítási forma, amit követően úgy lehet műveleteket végezni az adatokkal, hogy azok mindvégig titkosítva maradnak.



1. ábra Hawk-modell: aukciós séma  
(Forrás: saját szerkesztés)

Ezek alapján beláthatjuk, hogy az üzleti életben megkerülhetetlen a Hawk-modell, hisz a könyvelési rendszerekben gyakran szükség van rá, hogy a tranzakciók érvényességét ellenőrizzük, de azok érzékeny részleteinek ismertetését minimalizáljuk. A tranzakciók titkosított formában kerülnek rögzítésre, miközben a blokklánc hálózat validálja ezek érvényességét.

## 5. BLOKKLÁNC ÉS KÖNYVELÉS

### 5.1. KÖVETKEZŐ GENERÁCIÓS APPLIKÁCIÓK

A blokklánc működésének és előnyeinek megértése után, bátran kijelenthetjük, hogy a fenti példák csupán egy vékony szeletét jelentik a blokklánc könyvelésben való felhasználásának. Sean Stein Smith részletesebben is foglalkozik azzal, hogy milyen hatásai lennének a blokklánc technológia bevezetésének a könyvelési, pénzügyi és könyvvizsgálati folyamatokra. (Stein Smith, 2018)

Fő jellemzőiben Sean Stein Smith is a biztonság, átláthatóság és adatintegritást látja: az automatizált tranzakciókezelés minimalizálja az emberi hiba (vagy csalás) lehetőségét. Meglátása szerint a „következő lépés” az okos szerződések rendszeresítése, és bevezetése, amivel nem csak a pontosság és biztonság növelhető, de az adatfeldolgozás sebessége is. Ennek köszönhetően a riportok és jelentések azonnal és hitelesen elkészíthetők lennének, hisz a tranzakciók szinte azonnal rögzülnek a hálózaton, és az okos szerződéseknek hála az adatokhoz valós időben lehet hozzáférni.

A valós idejű adatokból következik, hogy a vállalatok könnyebben és pontosabban tudnak megfelelni a törvényi követelményeknek, ami hatalmas terhet venne le a vállalkozásokról, és rengeteg emberi erőforrást szabadítana fel, amit aztán hasznosan tudnának a rendszerbe visszaforgatni: a könyvelők és pénzügyi szakemberek sokkal inkább koncentrálnának az értékelésre, elemzésre és döntéshozatal előkészítésére, miközben az eddigi operatív lépéseiket a technológia hajtja végre.

- **Valós idejű adatok:** Smith szerint a blokklánc technológia segítségével a könyvvizsgálók és elemzők közvetlen hozzáférést kapnak az aktuális pénzügyi tranzakciókhoz és adatokhoz. A blokklánc egy valós idejű, idősorosan rendezett főkönyvet biztosítana, így a lehetséges hibák (vagy szabálytalanságok) azonnal észlelhetők lennének: az eddigi retrospektív könyvvizsgálati modellt egy proaktív, folyamatában történő megközelítés váltaná.
- **Automatizált ellenőrzési folyamatok:** A dolgozatban többször is szó esett arról, hogy a tranzakciók a blokkláncon egymásra és egymásba épülnek az adatok hashlésével, és azzal, hogy az adott blokk mindig az előző blokk végével kezdődik. Így a könyvvizsgálói folyamatok egy része leegyszerűsíthető azzal, hogy a rendszer ön-

állóan képes az adatok integritását és pontosságát vizsgálni, ezzel jelentősen csökkenteni az audit átfutási idejét. Az automatizálás nem csak időt, hanem pénzt is spórol, hisz egy auditálás költségeinek jelentősé részét teszi ki az adatgyűjtés és azok validálása, hitelességüknek ellenőrzése.

- **Harmadik fél általi ellenőrzés:** A technológiának köszönhetően a harmadik fél (hatóságok, független könyvvizsgálók) könnyebben férhetnek hozzá, megfelelően hitelesített (és védett) adatokhoz, így a különböző compliance ellenőrzések egyszerűbbé és gyorsabbá válnak, mivel az adatok közvetlenül, megbízható forrásból származnak és nem igényelnek további ember által végzett dokumentum-ellenőrzési lépéseket.

## 5.2. KIHÍVÁSOK

Természetesen, ha a technológia előnyeiről beszélünk, úgy meg kell említenünk a jelenlegi kihívásait is, hiszen jogosan tenné fel az ember a kérdést, miért nem implementálta még teljes egészében senki? A BigFour (Deloitte, EY, KPMG, PWC) mindegyike foglalkozik a témakörrel és a blokklánc hasznosításával, bár különböző mértékben. Példának okáért a JP Morgan a saját érdekeltségei a Quorum rendszerét használják (ez több száz leányvállalatot jelent), míg a Deloitte vagy a PWC az IOP rendszereit. Mindkettőre igaz, hogy főképp Amerikában, mivel az európai GDPR szabályozások még tisztázatlanok, és sokkalta bürokratikusabb térség, mint az amerikai.

A hármas könyvelés blokklánc alapú modelljének még 2024-ben is rengeteg kihívással kell szembenéznie, többek közt technológiai, szakmai kompetencia-béli, vagy épp szabályozási és jogi aspektusokkal.

### 5.2.1. Technológiai kihívások

A blokklánc technológia egyik problémája, hogy a tranzakciós kapacitásuk korlátozottabb, mint a hagyományos centralizált rendszereké: egy-egy hálózat (Bitcoin, Ethereum) maximum pár ezer tranzakció elvégzésére képes másodpercenként. Ez jelenlegi felhasználási keretek között működőképes lehet, hiszen amíg az adatbevitel humán erőforrást igényel, addig még sokáig nem fogjuk utolérni a technológia kapacitásának határait. Könyvelés területén kijelenthetjük, hogy hatalmas tranzakció számnak kell történnie ahhoz, hogy a kapacitás határt elérjük, de fontos tényezőként kell ezt is kezelni.

Nem véletlen ezeknek a hálózatoknak az egyik legfőbb metrikus adata, a TPS (azaz transaction per second), és nagy verseny folyik jelenleg is, hogy melyik hálózat, mekkora kapacitás

növelést tud elérni.<sup>8</sup> További kihívást jelent a konszenzus mechanizmusok skálázhatósági problémája: jelenleg a gyakran használt „proof of work” mechanizmus lassú, és nagy számítási kapacitást igényel, nem beszélve a magas energiafogyasztásról. (Ez a mechanizmus használatos a bitcoin bányászat során.)

Emellett kísérleteznek már egy másik, skálázhatóbb mechanizmussal, a „proof of stake” - kel, de Belluci és társai szerint, még ezek az alternatív mechanizmusok sem tűnnek – egyelőre – teljesen mértékben megfelelőnek (Belluci, Bianchi, & Manetti, 2022).

Technológiai kihívásként jelentkezik az adatfeldolgozási és tárolási erőforrások szűkössége: szintén kihívás elé állítana bármilyen nagy céget, a jelenlegi konszenzusmechanizmusok mellett.

### **5.2.2. Adatbiztonság és adatvédelem**

Bár az adatbiztonságról és adatvédelemről a dolgozat során többször is pozitív értelemben esett szó, mégis meg kell vizsgálni egy másik aspektusból is: mivel a blokklánc technológia egy megmásíthatatlan főkönyvet hoz létre, így minden egyes tranzakció örökre rögzítve marad, ami egyfelől előnyös a megbízhatóság és nyomon követhetőség szempontjából, de másrésről problémás lehet a jelenlegi adatvédelmi előírások és GDPR szabályzások világában, hogy meddig, hogyan és ki által tárolható egy adat.

Különösen kérdésessé válik, hogy amennyiben hibásan kerül rögzítésre egy tranzakció, úgy hogyan lehet azt javítani, illetve a blokkláncon tárolt érzékeny adatok bár védve vannak, de amennyiben ez a védelem nem megfelelő, úgy ki a felelős az adatokért. A GDPR és a decentralizált adatbázisok, rendszerek összeegyeztethetőségét az Európai Parlament is folyamatosan vizsgálja.

#### **5.2.2.1. Megváltoztathatatlanság és a GDPR összeférhetlensége**

A törléshez való jog, a GDPR egyik alapjoga, miszerint az egyének jogosultak arra, hogy kérvényezzék személyes adataik törlését, ha azokra már nincs szükség, vagy más okból indokolt.

---

<sup>8</sup> Az Ethereum jelenleg az irreálisan nagy ugrásnak tűnő, 100 000 TPS-t célozta be (Sergeenkov, 2024).

Mivel a blokklánc technológia egyik alapelve a tranzakciók megmásíthatatlansága és örök érvényű rögzítése, ez kérdéseket és problémákat vethet fel, amit minden technológiai, mind jogi oldalról ki kell vizsgálni. Emellett a helyesbítés joga is kérdőjelessé válik, hisz a blokkláncon az előzőleg hibásan rögzített adat csak további új adatokkal korrigálható, de a hibás adat így is megtalálható marad a rendszerben. (Fink, 2019)

#### **5.2.2.2. Adatkezelői és adatfeldolgozói felelősségek**

A GDPR előírja, hogy minden személyes adatot kezelő szervezet egyértelmű adatkezelői vagy adatfeldolgozói szerepet tölt be, és felelősséget vállal az adatok védelméért. A blokklánc decentralizált jellege azonban megnehezíti annak a megállapítását, hogy ki a felelős az adatok védelméért, kezeléséért és adatvédelmi incidensek kezeléséért. Például ki a felelős akkor, ha egy blokklánc tárolt adat kompromittálódik? Melyik résztvevő vagy csomópont a felelős érte?

Az adatvédelemért felelős szereplők azonosítása bonyolult, mivel több, egymástól független szereplő is részt vesz ebben. A központosított adatrendszerek esetében az adatkezelők és feldolgozók könnyen meghatározhatóak, míg a decentralizált rendszerben az adatok minden résztvevő tárolja és frissíti, így a felelősség kérdését jogilag tisztázni kell.

#### **5.2.2.3. Érzékeny adatok védelme és adatbiztonsági kérdések a technológia függvényében**

Bár a rendszer rendkívül erős kriptográfiai megoldásokkal operál, nincs olyan kriptográfia, ami előbb vagy utóbb ne lenne visszafejthető. Általános kritika a rendszerrel szemben, hogy jelenleg rendkívül erős titkosítást jelent, de nem tudhatjuk, hogy 5-10-30 év múlva milyen módon lehet visszafejteni ezeket az adatokat. Jelenlegi számítási kapacitások mellett a blokklánc hálózatok teljesen biztonságosak, viszont a kvantumszámítógépek megjelenésével újabb kérdések merülnek fel a hálózat biztonságát illetően. Amennyiben a blokklánc technológia lépést tart a kvantumfejlesztésekkel, akkor is további kihívást jelent, hogy a régebbi blokklánc technológiával tárolt adatok is titkosítva legyenek, és egy újabb technológiával se legyenek visszafejthetők.

#### **5.2.2.4. Megoldási kísérletek, megkerülési lehetőségek**

A fenti kérdések természetesen már mind a törvényhozókat, mind a fejlesztőket foglalkoztatják, így már több lehetséges válasz is létrejött ezekre a kihívásokra. Többek közt ilyen megoldást jelenthet egy „on-chain/off-chain” rendszer, ahol a kompatibilitás érdekében a

blokkláncon csak a feltétlenül szükséges adatokat (hashek, azonosítók) tárolnak, míg az érzékeny adatokat továbbra is off-chain (láncon kívül) adatbázisokban tárolják, így a blokklánccs csak a minimális, megmásíthatatlan információkat tárolja el, az érzékeny adatok pedig megfeleltethetők maradnak a GDPR-nak. Az off-chain adatbázisban tárolt adatok hashei összeegyeztethetők az on-chain tárolt hashekekkel, így a blokklánccs csak egy hitelesítő főkönyvként működne, azon teljes értékű adatrögzítés nem történne. Az off-chain adatbázis hitelességét a megmásíthatatlan főkönyv garantálná, amennyiben eltérés adódna, úgy további könyvvizsgálatra lesz szükség.

A gyakorlati haszna a rendszernek, hogy érzékeny adat sosem kerül a blokklánccra, így az a későbbiekben könnyedén módosítható egy újabb blokkal és bejegyzéssel, ami hitelesen magyarázza azt, hogy az off-chain adatbázisból miért hiányzik az adott hash-hez köthető sor. (Vagy miért tér el.) A rendszer fontos része, hogy a végfelhasználónak, azaz annak, aki az adatot szolgáltatja (adminisztrátor, könyvelő stb..) mindenképp saját aláírásával kell azt rögzítenie, hisz a belépési ponton már megkérdőjelezhetetlennek kell lennie az adatbevitelnek a rendszer integritásának érdekében. (Ez lehet egy böngészőbe épített modul, hardverkulcs vagy akár az e-személyi rendszerrel összekötve.)

Sokat tárgyalt megoldás, az előzőleg már említett „Zero-knowledge proof” technológia és a Hawk-modell, ami lehetővé teszi, hogy bizonyos információkat úgy igazoljanak, hogy azoknak tényleges tartalmát nem fedik fel, így csökkenthető a blokkláncon tárolt érzékeny adatok mennyisége.

### **5.2.3. Interoperabilitás**

A meglévő rendszer közel 600 éve szerves részét képezi a könyvelés világának és a 600 év alatt is átesett a saját evolúcióján, ahol a menetközben felmerülő újításokat – lévén, hogy a rendszeren belül maradtunk – könnyű volt integrálni. Mind Smith, mind Bellucciék foglalkoznak azzal a problémával, hogy hogyan lehetne egy ennyire új rendszert, a meglévő komplex, globális rendszerbe átültetni.

A blokklánccs rendszerek által használt adatstruktúrák gyakran eltérnek a centralizált adatbázisokétól, így hatalmas kérdést vet fel, ezeknek a rendszereknek a szinkronizációja, össze-

illesztése. Az adatkonzisztencia fenntartása szintén kérdés lenne, hisz a blokklánc rendszerben a különböző csomópontoknak azonos adatokat kell kezelniük, ami csak akkor lehetséges, ha a meglévő rendszerek szinkronizálva vannak.

Ha egy vállalat több pénzügyi platformot használ, úgy minden egyes rendszert szinkronizálni kell, hogy mint teljes egész működhessen. Ezt követően az adatbevitel lesz a legnagyobb hibaforrás: mivel a rendszerben tárolt adatok megmásíthatatlanok, minimalizálni kell az adatbevitel lehetőségét. A cégeknek egy merőben új rendszer implementálásánál nem csak rengeteg költsége keletkezne (hardver- szoftverinfrastruktúra, átképzési költségek stb.), de a hiba nélküli kivitelezése akár több éves projekt is lehet.

További kihívás elé állítja a modellt, hogy a különböző blokklánc hálózatok is más technológiai alapon működnek, és gyakran nem képesek közvetlenül egymással kommunikálni: mindegyik rendszer saját protokollal, adatstruktúrával és konszenzus mechanizmussal rendelkezik, amelyek közti átjárás jelenlegi technológiai szinten még nem megoldott, viszont a rendszer alkalmazásához elengedhetetlen feltétel (Stein Smith, 2018).

#### **5.2.4. Implementációs költségek**

##### **5.2.4.1. Hardver és szoftverinfrastruktúra költségek**

A blokklánc technológia implementálása jelentős beruházásokat igényel mind hardveres, mind szoftveres infrastruktúra terén. A hagyományos pénzügyi rendszerekhez képest a blokklánc által használt decentralizált hálózati struktúra sokkal nagyobb számítási kapacitást és modernebb biztonsági mechanizmusokat követel meg. Ez vonatkozik a fizikai szerverekre, adatközpontokra, de még a különböző blokklánc platformok licenz és karbantartási költségeire is. Ezek a költségek a kis- és középvállalkozások számára különösen nagy pénzügyi terhet róna, miközben korlátozott költségvetéssel rendelkeznek (Belluci, Bianchi, & Manetti, 2022).

##### **5.2.4.2. Oktatási, átképzési költségek**

Belluciék munkájukban felhívják a figyelmet arra, hogy a technológia implementálása megköveteli, hogy az alkalmazottak rendelkezzenek a rendszer működéséhez szükséges technikai tudással. Ez további továbbképzési költségeket és kihívásokat eredményezne, mivel a jelenleg számviteli szakemberek nem feltétlenül rendelkeznek a blokkláncához kapcsolódó

speciális ismeretekkel. Természetesen a számviteli dolgozóknak nem kell a titkosítás pontos mechanizmusát ismerniük, ellenben egy átfogó oktatási program (blokklánc alapjai, biztonsági mechanizmusok alapjai, adatkezelési protokollok stb.) akkor is szükség lenne, hogy a rendszert teljeskörűen és magabiztosan használhassák a pénzügyi végzettséggel rendelkező felhasználók.

#### **5.2.4.3. *Időigényesség költsége***

Mind Smith, mind Belluciék kiemelik, hogy a rendszer komplexitása miatt, annak integrálása meglévő vállalati rendszerekbe, nem csak költséges, hanem időigényes is.

A pénzügyi, számviteli szektorba való implementálás különösen nehéz, mivel a tranzakciós adatokat egy precizitással és pontosan kell kezelni, míg biztosítani kell, hogy a rendszerek folyamatosan működjenek, még az implementálás alatt is. Ez a pénzügyi intézményeknek kifejezetten nagy kockázatot jelent, mivel akár több éves átalakítási projekt is lehet, miközben az üzletmenet folytonosságát fent kell tartaniuk, ami növeli a költségeket, hisz egyszerre kell a meglévő rendszert finanszírozni, miközben az új rendszert kiépítik. Ez egy további visszatartó erő a nagyvállalatok számára, hisz a meglévő rendszerek stabilan működnek, és a szektor konzervatív jellegéből fakadóan, a vállalatok csak akkor vállalkoznának ilyen jelentős strukturális átalakításra, ha a rendszer valóban megbízhatóan, pontosan működik, és bizonyíthatóan költséghatékonyabb.

## 6. HÁTTÉRINTERJÚK

Mivel szűk hazai szakirodalom állt rendelkezésre a dolgozat készítéséhez, így a primer kutatás során hazai, magyar szakembereket kérdeztem a hármas könyvelést illetően. A téma összetettségét tekintve, a három interjú lefedi a rendszert: Vidákovics Attila, a DLabs Kft. cégvezetőjeként, mint blokklánc technológiai szakember a technológia oldaláról, Szabó Péter a Soneas Vegyipari Kft. számviteli munkatársa a könyvelés és számvitel oldaláról, míg Zsoldos László, az OTP Bank Nyrt. munkatársa a pénzügyi- banki világ oldaláról osztotta meg a tapasztalatait. A következő interjúkban az általam felvázolt problémákat **kiemeltem**, majd ezt követően az interjú alanyok válaszai kerülnek bemutatásra. A kiértékelést, a levonandó tanulságokat a dolgozat Konklúzió része tartalmazza.

### 6.1. INTERJÚ VIDÁKOVICS ATTILÁVAL- DLABS KFT - 2024.11.11

**Magyar nyelvű kutatást, felhasználást nagyon keveset találtam, és mindenhol abba futottam bele, hogy az elképzelés jó, és még a Big4 is kutatja, de a technológia egészében még nincs kiforrva és sok kérdést hagy maga után: egyrészt skálázhatósági kihívásokkal küzd, másrészt a GDPR szabályozások is kihívások elé állítják.**

Teljesen kiterjedten mindenre még nincs megoldás, viszont vannak olyan szolgáltatások, a JPMorgan például saját érdekeltségeinek – közvetlen több, mint 400 leányvállalat – a Quorumot használják, egy saját blokklánc fejlesztést, ahol nem csak értéket mozgatnak, hanem elsősorban dokumentum hitelesítésre használják. A Deloitte és a PWC nem csak kutatja, de például az IOP rendszerét használja is ilyen téren.

Az európai jogszabály még készülöben van, hogy mit lehet hitelesnek és hitelesítettnek minősíteni ilyen módon, az amerikai piacon viszont ez kevésbé szabályozott, így ott már élesebben használják. Az Európai Unió ilyen szempontból kissé bürokratikusabb térség, de ennek ellenére már dolgoznak a szabályozásán, de ez viszonylag centralizálná az adatokat, akár bizalmas adatokat, ami nem mindenkinek tetszik, mivel pont a decentralizáltságot adná fel.

**Belluciék tanulmányában találkoztam egy teóriával, megoldásötlettel, miszerint az adatvédelmi kihívásokat egy on-chain/off-chain rendszerrel lehetne kivédeni, ahol az érzékeny adatok off-chain egy klasszikus adatbázisba kerülnek, míg a kevésbé érzékenyek pedig on-chain közvetlenül a blokkláncra.**

Ez a megszokott megoldás. Technológiai szempontból már találkoztam vele, de élő megoldásban még nem találkoztam olyannal, hogy a kontrakton belül az érzékeny adatot titkosították volna, ezt általában off-chain szokták megoldani, egész egyszerűen egy hash-sel pedig rögzítik a blokkláncon, így nincs semmilyen érzékeny adat a láncon, viszont össze lehet matchelni az off-chain adatbázissal. Meg lehetne oldani on-chain az egészet, de nagyon sok adatot kellene mozgatni, ezért ezt megpróbálják elkerülni, mert egyszerűbb – adatbiztonsági szempontból is – ha külső adatbázisban vannak az érzékeny adatok. Bizalmi szempontból ennek nincs hátulütője, mert ha az adott dokumentum/tranzakció hashe a blokkláncba van rögzítve, azzal visszaélni nem lehet, viszont az off-chain adatbázis validációjára használható marad. Egy dolog tud megtörténni: eltűnhet adat.

### **Mármint?**

Hogy, ha ez egy off-chain adatbázisban tárolt adat, és onnan valaki valamit el akar tüntetni, az továbbra is lehetséges. Ez egy általános kritika szokott felmerülni ez ellen a megoldás ellen.

**Tehát, lényegében ez a módszer működhetne úgy, hogy a blokklánc mint egy validáló lánc kerül felhasználásra, amivel az off-chain adatbázis hitelességét lehet vizsgálni, ha ott eltérés van a blokkláncához képest, akkor vizsgálatra van szükség?**

Igen, akkor innen lehet tudni, hogy ott valami történt (hiba vagy szándékos megmásítás, törlés). Ez tervezés kérdése, hogy mi az, ami rögzítésre kerül a blokkláncon, időbélyeg, dokumentum típus, csak az érzékeny adatokat kell off-chain tárolni. Tehát ezekben a megoldásokban van realitás, például a magyar e-Diploma rendszer is így működik. Ott sincs a diploma a blokkláncon tárolva, csak annak a hashe. A blokklánccal lehet vizsgálni az eredetiségét: ki írta alá, ki rögzítette, ki módosította stb.

**A hipotézisemben az egyik gondolat az, hogy nem csak átláthatóbb lenne a könyvelés, hanem nagyon sok erőforrást szabadítana fel a rendszer...**

Igen, ezt lehet automatizálni ugyanúgy, mintha on-chain lenne minden. Lehet titkosítani a láncon is az adatokat, technológiailag megoldható, de egyelőre számomra nem ismertek olyanok, akik ezt választották volna.

**Bár a kriptográfiai megoldások erősek, és mai fejjel – hardverrel – majdnem visszafejthetetlenek, de nem vet fel kérdéseket, hogy minden érzékeny adat publikus láncon elérhető?**

Az szokott lenni a kritika, hogy most ez jól működik, de ki tudja, hogy 3-5-10-30 év múlva, milyen módon lehet visszafejteni, megnézni ezeket az adatokat. Ha ott van a blokkláncon, később ezek akár napvilágot is láthatnak. Ellenben, ha csak a hashek vannak ott, arról azt

feltételezi a szakma, hogy amennyiben elég magas bitszámú hasht használnak, az több évtizedig biztosan nem lesz visszafejthető, csak találgatással. De annak az energia- időfelhasználása irreálisan magas. A hash feltörésén túl, vannak más olyan technikák is, amivel ezt nehezíteni lehet, például egy image fájl – kép – elrejtése a dokumentumban. A szakemberek általában 30 évre szokták megbecsülni egy kriptográfiai megoldás élettartamát.

**Gondolom, amennyiben menetközben észrevennék, hogy közeledünk ahhoz a ponthoz, hogy ne legyen többé biztonságos és migrálnánk a rendszer off-chain, azzal már elkészénénk?**

Igen, főképp, hogy a blokkláncunkról lehet akárkinek másolata még a migráció, vagy update előttről, és nyugodtan visszafejthetné azt, hiába titkosítottuk a live-verziót tovább, vagy migráltuk off-chain.

**A meglátásom szerint, az egész folyamat automatizálni lehetne a könyvvizsgálást egészen addig a pontig, amíg a hashek egyeznek, és a könyvvizsgálóknak csak ott kéne manuálisan belépniük, ha eltérés van az on-chain/off-chain hashei közt.**

Teljes mértékben elképzelhető, és a szakembernek nem kell értenie a technológiához. Ehhez kell egy olyan rendszer, ami felhasználóbarát módon kínálja a felületet hozzá. Egy felületen „nyomkodja” a megszokott módon, a háttérben pedig a rendszer dolgozik a kriptográfián és azon, hogy minden a helyére kerüljön. Fontos, hogy azért minimális szinten értse a rendszert, de ez egy pár napos átképzés keretében megoldható. Fontos, hogy hitelesen tudjon aláírni, akár egy böngészőbe épített modulon keresztül, egy hardverkulcs vagy akár e-személyivel összekötve, mert minden adat bevitelhez fontos, hogy hozzá lehessen kötni, hogy ki végezte azt el, ezzel alapjaiban biztosítva a rendszer hitelességét a „belépési ponton”. Adatot változtathat, de azt megint alá kell írnia.

**Egy javításnál új blokk jön létre, de attól még a régi blokk létezni fog, ez nem jelent adatvédelmi gondokat?**

Ezért szokták azt választani, hogy a blokkláncon csak hasheket és eseményeket rögzítenek, ahol az esemény leírhatja, hogy ott törölni/változtatni kellett valamit, így ez jelezve van, hogy van egy dokumentum hash, ami törölve/változtatva lett (miért, ki, mi alapján, mikor csinálta), így az off-chain adatbázisból eltűnik, az on-chain adatok közt pedig nem is került rögzítésre érzékeny adat. (Csak hash és esemény). Ki lehet törölni, de így rögzítve lesz, hogy ki és miért törölte.

**Beszéltünk arról, hogy megoldható a rendszer automatizálása. Van realitása egy olyan automatizálásnak, ahol a smart contractokon keresztül, például egy vásárlásnál a vá-**

**sárló fél letétbe helyezi a vásárlás összegét, addig a pontig, amíg a rendelt áru kiszállításra nem kerül, és a raktári átvétel során, miután megerősítik az áruátvételt, a smart contract automatikusan elutalja a letétbe helyezett összeget? Így lényegében mindkét fél bebiztosítaná magát, hogy csak akkor történik meg a tranzakció, ha a másik fél is teljesítette a rá eső részt?**

Teljes mértékben. Vannak olyan működő rendszerek, ahol még az eladó fél is letétbe helyez összeget a smart contracton, amivel biztosítani tudja a vásárló felet arról, hogy a lehető leggyorsabban fogja teljesíteni a szerződést. (Magyarul nem érné meg neki késlekedni, hisz a saját pénze is letétben van addig, amíg nem teljesít.)

**Jelenlegi technológiai állás mellett, mennyire lenne az adatok rögzülése valósidejű?**

Ma már azért sokkal modernebb rendszerek vannak, mint a bányászat elején, úgyhogy ennek tekintetében nincs akkora aggodalom, mint a skálázhatósággal kapcsolatban. Vannak természetesen elméleti problémák, ahol ez bonyodalmat okozhatna, de egy általánosan nagy, több ezer embert foglalkoztató cégnél úgy, hogy emberek viszik fel az adatokat, nem fogják a technológiai határokat utolérni. Más lenne ez akkor, ha több millió önvezető autónak a másodpercenkénti 30-40-50 adatáról lenne szó, de amíg humán forrásról beszélünk, addig a mai rendszerek már versenyképesek.

## **6.2. INTERJÚ SZABÓ PÉTERREL - SONEAS VEGYIPARI KFT. - 2024.11.14**

**Jelenleg kettős könyvelést használnak világszerte, viszont a blokklánc megjelenésével több elképzelés is van a könyvelés forradalmasítására. Hogy látnád a technológia felhasználásának előnyeit a pénzügy-számviteli területen?**

Én azt gondolnám, hogy ha könyvelésnél blokkláncról beszélünk, akkor nem az a fő aspektus a fontos, hogy mindörökké fennmaradjon és változatlan maradjon, sokkalta inkább a tranzakciós része. Egy adott tranzakcióval minimum 4 szereplőnek foglalkoznia kell (adó, vevő, hatóság, könyvvizsgáló), és ez jelenleg rengeteg munkát jelent. Egyetlen tranzakciót mindkét félnek el kell könyvelnie a megfelelő számlaosztályon, annak értelmezéséhez hozzáférést kell biztosítani a hatóságok és könyvvizsgálók részére – a törvényi kereteken belül -. De ez tovább bővíülhet további szereplőkkel, akiknek ezekkel munkájuk lehet. Komplet csapatok dolgoznak azon, hogy minden adat a helyére kerüljön, és a jelenlegi adatmennyiségek mellett ez egy hatalmas, véget nem érő munka, ahol nem ritka, hogy hónapzáráskor még be se érkezett az adott időszakra szóló számla, így trükközni és ügyeskedni kell, hogy mit hova tegyünk.

Ebben látnám a legfőbb előnyét a rendszernek, hogy minél több részfeladat, feladat automatizálható legyen.

**Mennyiben befolyásolná a könyvelői-számviteli munkaköröket, ha ez a rendszer olyan szinten lehetne automatizálható, hogy egy adott tranzakció akár napon belül rögzítésre kerüljön?**

Ha azt mondhatjuk, hogy egy adott tranzakció adott napon belül lesz elkönyvelve, az már hatalmas áttörés lenne a szakmának.

Gyakorlatban ez úgy néz ki, hogy könyvelők és könyvelőasszisztensek munkájának 80-90%-a az, hogy ezt az adatrögzítést elvégezzék. Van egy másik rétege ennek az egésznek, hogy a felvitt adatoknak az ellenőrzése, értelmezése, jóváhagyása az már inkább kontrolling területnek minősül, de így jóval több humán-erőforrás maradna erre. Egy ilyen automatizáció a könyvelés szakmának hatalmas részét kiváltaná. Egy cég például feldolgoz egy hónapban 1000 számlát, amiből legalább 200 a mai napig postán érkezik, ezt egy titkárnak be kell szkennelnie, elküldeni, szakembernek ellenőrizni, rögzíteni, osztályozni és rendszerezni. Egy számla akár 4-5 emberen is átfuthat.

**Ha ennyi energiát felszabadítunk, tudnák ezt szakmai kompetenciáiknak megfelelően másra fordítani?**

Természetesen. Ha ez a repetitív, adminisztratív munkateher megszűnne, úgy egy könyvelői, számviteli csapat részletesebben foglalkozhatna a tartalmi résszel, a minőséggel, de sajnos jelenleg a szakma – emberhiány és a rengeteg adat miatt – ott tart, hogy a mennyiség a minőség felett van, így minőségi szempontból ez hatalmas előrelépés lenne. Rengeteg shared service centerbe vonják össze ezeket a munkákat jelenleg, ahol erre specializálódott emberek foglalkoznak a számlák feldolgozásával, mivel ez jóval költséghatékonyabb, de ez egyértelműen a minőség rovására megy. De akár sokszor az adminisztratív munkák nagyrészt kiszervezik a harmadik országokba, ahol betanított munkások rögzítenek, de itt is érezhetjük a minőséget övező veszélyt.

Ez egy létező igény a cégek részéről, hogy minél több dolgot lehessen automatizálni, egyszerűsíteni, de közben a minőség rovására ne menjünk. Tehát a felszabaduló „szabadidőt” pontosan arra lehetne fordítani, hogy a minőséget javítsuk. Mondok egy példát: anyagköltség, ha veszünk egy anyagot, bekerül a raktárba, és anyagköltségként kerül könyvelésre, de vannak olyan specifikus cégek, sajátosságok, ahol nem tudod ilyen egyértelműen kezelni ezeket az adatokat, például folyékony nitrogén fogyasztásának könyvelését nem tudod ilyen egyszerűen mérni és könyvelni, így sokszor ezek nincsenek is készletre véve, hanem beérkezéskor leírják költségként, hisz nem lekövethető fizikailag. Ilyen sajátosságokhoz emberi

szemre és szakképzett dolgozóra van szükség. Vagy az óvatosság elvét követve nem mutathatunk ki olyan követelést, ami kockázatos, hogy be tudjuk-e hajtani vagy sem. Ennek értékelése kevésbé automatizálható, hisz humán interakcióra, elemzésre és döntéshozatalra van szükség.

Ha minőségről beszélünk, akkor például hasonló példákra gondolhatunk. Maga a számvitel műfajról sokan azt gondolják, hogy egzakt, de rengeteg tér van a mérlegelésre, amiben jobban kihasználhatnák a képzett szakemberek a kompetenciáikat, mintsem az adminisztratív munkában.

**Adatvédelmi szempontból milyen aggályokat látsz számviteli szakemberként abban, hogy tranzakciók adatai nyilvános blokkláncon legyenek – még ha titkosítva is – elérhetőek?**

A GDPR és bizalmas adatok kezelése hatalmas kérdés lehet a blokklánc felhasználása során. Fontos elhatárolni a GDPR szempontjából érzékeny adatot és az üzleti érdeket tekintve érzékeny adatokat. A könyvelés már a mai nap is viszonylag jól tudja kezelni az érzékeny személyes adatokat, hisz például egy bérköltség fizetése során is, az adatokat már aggregáltan kapják, így személyes adatokat már ők sem látják, de természetesen elképzelhető az, hogy a munkájuk során igen is rögzítésre kerülnek hasonló adatok.

Sokkal nagyobb kockázatnak érzem azt, hogy egy kiállított számlából milyen adatok kerülhetnek fel a blokkláncra, hisz nem szeretnénk, ha a konkurencia számára minden tranzakciónk, beszerzésünk értéke nyilvános lenne.

### **6.3. INTERJÚ ZSOLDOS LÁSZLÓVAL - OTP BANK - 2024.11.13**

**A dolgozatom témája a hármas könyvelés blokklánc alapon, ez egyelőre még tudtommal gyakorlatban csak részben van megvalósítva, de teljes rendszer még nincs adaptálva sehol, kisebb részeket cégeken belül már felhasználnak.**

Tudomásom szerint, a legális vagy valós pénzügyi intézeteknél kizárólagosan nincs alkalmazásban, de maga a bitcoin, vagy hasonló coinok kereskedésének a könyvelése, mind blokklánc alapon megy. Ilyen értelmezésben, élesben van használva.

**A jelenleg használt kettős könyvelésben azért van csalás lehetőség, mert a két főkönyv (két cég) közt nincs kapcsolat, illetve ami van, az a könyvvizsgálás. A teória szerint, ha lenne egy blokklánc hálózat a kettő között, a tranzakciók mindkét főkönyvben szerepelnének – mint eddig is – viszont egy hash lenyomatként szerepelne a publikus blokkláncon, és ez hitelesítő főkönyvként tudna működni.**

A klasszikus főkönyv, arról szól, hogy publikusak a szereplők, de maguk a tranzakciók nem publikusak, azokat mindenki a saját főkönyvébe könyveli. Az, hogy ki hogyan és hova könyveli le, az már másik kérdés. A blokklánc történetében megfordul a dolog: a szereplők titkosak, és a tranzakciók nyilvánosak. Ezt a nyilvános tranzakció halmazt tárolja a blokklánc, ami egy több szereplő által replikált adatbázis. Mivel mindenkinél meg van ez a közös főkönyv, így a rendszer észleli azt, ha bárhol adatmódosítás történne. Ha bárhonnán adat tűnne el, az a többi szereplő részéről pótolható.

### **Vannak erre egyéni törekvések vállalaton belül?**

Van már több házon belüli fejlesztés jelenleg is, még ha nem is a blokklánc könyvelés alapú használatát illetően, de a blokklánc, mint technológia nagy figyelmet kap. Az új technológiák felhasználása egy eléggé fókuszált terület, nem csak nálunk, de minden pénzügyi intézetnél már több éve.

### **Egy ilyen rendszer implementálása mekkora teher lenne egy cégnek?**

Egy-egy ilyen alkalmazás fejlesztés költsége a csillagos ég lehet, főképp a járulékos, migrációs költségeket figyelembe véve. Nem lehet ezt egyértelműen egyoldalúan csinálni. Ez az egész blokkláncos történet úgy működik, hogy benne vagy egy „IT-buborékban” amit, ha nem mindenki használ, akkor egy féloldalas sztori lesz belőle. Példának okáért a bitcoinnál is most kezdődik el egy világszintű elfogadottság, mert a bankok elkezdenek beszállni a legitimációjába, de ennek ellenére egy világszintű banki-bitcoin rendszer (elfogadottság) nem készült el, viszont mindenki készül rá. Tehát nem elég, hogy egy vállalat implementálja a technológiát, széleskörű elfogadottságra van szüksége a működéshez.

### **Állami szinten van érdeklődés, vagy érdek, hogy lépés tartsanak hasonló technológiai fejlődésekkel?**

Nyolc évvel ezelőtt az, hogy felhőben tároljunk adatokat nagyon sok ellenállásba ütközött. Az, hogy egy olyan infrastruktúrát használjunk üzleti célra, ami nem az enyém, az egy nagyobb csuklást eredményezett. Adatvédelmi, IT-biztonsági, ellenőrizhetőségi vonatkozásokban nagyon sok kérdést vetett fel. Ehhez képest, azt láttuk az elmúlt 10 évben, hogy állami szinten – Magyar Nemzeti Bank – kezdik úgy módosítani a szabályozásokat, és adnak ki különböző ajánlásokat, hogy ezt a felhő alapú működést kezelhetőbbé tegyék, és elfogadhatóvá definiálják. Különböző ajánlásokkal segítenek központilag, hogy milyen adatvédelmi, tárolási és IT megfelelési szabályokra figyeljenek a vállalatok, ha felhő alapra akarnak áttérni, ezzel segítve a technológia implementálását. Ha például adatvédelemről beszélünk, felmerül a kérdés, hogy melyik adatközpontot használja a vállalat? Az adatok

fölötti kontroll merőben függ a lokációtól, hisz más szabályozás alá esik egy amerikai vagy egy európai adattárolás.

**Akkor, ha jól értem, az állam próbálja segíteni a technológiai fejlődést a saját hatáskörében?**

Pontosan. Képes arra, hogy alá menjen, és biztosítsa azt a jogszabályi környezetet, hogy az újításokat legálisan lehessen használni. A blokklánc vonatkozásában ez kicsit hosszabb inkubációs időt igényel (hogy elfogadják), mert még sok vita van róla, hogy jó az alkalmazása a szektorban vagy sem, így az előértékelése még elhúzódik. Jelen tudomásom szerint még nincs központi ajánlás a blokklánc technológiát érintően.

## 7. KONKLÚZIÓ

A dolgozatban bemutattam a könyvelés történetét, és a ma használatos kettős könyvvitel kialakulását, míg ismertettem a blokklánc technológiai hátterét és annak előnyeit.

A hármas könyvelés blokklánc-alapú megközelítése egy megmásíthatatlan főkönyv ígéretével kecsegtet, de számos kihívással is szembe kell még néznie a jövőben.

A technológia lényege, hogy a tranzakciókat nem csak a résztvevő felek könyvelésében, hanem egy harmadik, blokklánc-alapú főkönyvben is rögzítésre kerüljenek, ami a blokklánc technológiának köszönhetően biztosítaná, hogy a rögzített adatok változtathatatlanok legyenek, így növelve a tranzakciós adatok integritását, ellenőrizhetőségét, csökkentve a hibák lehetőségét és csalások kockázatát. Ezen tényezők tekintetében megállapíthatjuk, hogy a hármas könyvelés sokkal magasabb fokú megbízhatóságot nyújt, mint a több száz éve használt kettős könyvelés. A jelenlegi technológiai szinten és jogi szabályozások keretén belül, a legelfogadottabb – és több nagy vállalat körében részben használt – megoldási mód, az on-chain / off-chain könyvelési rendszer, ami a régi centralizált adatbázisokban tárolná az érzékeny adatokat (így megfelelően a GDPR előírásoknak), míg a hozzájuk rendelt időbélyegeket és egyéb kevésbé érzékeny adatok hashét pedig a nyilvános blokklánc alapú főkönyvben. Ez lehetővé tenné, hogy az érzékeny adatok ne legyenek elérhetőek, változtathatóak és törölhetőek legyen a GDPR alapelvei szerint, míg a blokkláncon tárolt hasheknek köszönhetően minden egyes tranzakció és adat az adatbázisban automatizált módon ellenőrizhetővé válna, hisz amennyiben a hashek egyeznek, úgy az adatbázis pontos és sértetlen.

A megbízhatóság mellett az átláthatóság bizonyítása szintén célom volt: lehetőség adódhat a tranzakciók valós idejű nyomonkövetésére egy olyan megbízható főkönyvben, amihez az auditorok is hozzáférhetnek, algoritmusok által hitelesített tranzakciós adatokhoz. Ez különösen előnyös a könyvvizsgálat és a compliance szempontjából, mivel a folyamatok sokkal gyorsabbak és átláthatóbbak lehetnek a hagyományos könyveléshez képest.

Hatékonyságát tekintve a blokklánc-alapú könyvelés lehetőséget adhat a könyvelési folyamatok automatizálására, csökkentve az emberi beavatkozás szükségességét, és ezzel csökkentve a hibák lehetőségét. Mivel az adatok közvetlenül a főkönyvben rögzülnek, így elkerülhetővé válhat az adatok többszöri bevitele, és a manuális egyeztetés: az auditálási folyamatok felgyorsulnak. A megbízhatóság és átláthatóság magával vonzza az üzleti bizalom

erősödését is, hisz egy automatizált, algoritmikus alapon működő rendszerben többé nem az emberekben, hanem a matematikában kell megbízni.

A rendszer egyik legnagyobb előnye az automatizáció. Az okos szerződések használatával automatizált mechanizmusok építhetők be a rendszerbe, amik bizonyos tranzakciókat vagy műveleteket csak előre meghatározott események bekövetkezése esetén hajtanak végre. Az automatizálási lehetőségek csökkentik a humán erőforrás felhasználását, így a szakképzett számviteli és pénzügyi szakemberek a repetitív adminisztrációs feladatok helyett (adatbevitel, egyeztetések) értékteremtőbb feladatot végezhetnek el, mint például pénzügyi elemzések, jelentések készítése, stratégiai döntéselőkészítésben való részvétel.

Mindezek ellenére fontos kiemelni, hogy a technológia jelenleg rengeteg kihívással küzd. A jogi szabályozások még nem kiforrottak, és sok kérdést felvet a blokklánc-alapú adattárolás a GDPR alapelveinek tükrében.

Ki a felelős a tárolt adatokért? Hogy lehet érvényesíteni a „törléshez való jogot”? Hogy lehet érvényesíteni a „helyesbítési jogot”? Hogyan lehet meghatározni a klasszikus felelősségköröket, mint az adatfeldolgozó, és adatkezelő, ha ezeket automatizált rendszerek végzik? Mennyire lesz időtálló kiber- és adatbiztonsági szempontból a technológia?

Jelenlegi technikai szinten, a blokkláncon használt kriptográfiai megoldások még a legerősebb számítógépeknek is több száz évnyi számítással lenne csak feltörhető, visszafejthető, de a kvantumszámítógépek megjelenésével is lépést fog tudni tartani?

Természetesen nem csak jogi és adatvédelmi kérdések merülnek fel a technológia kapcsán, de a rendszer komplexitása szintén hatalmas kihívások elé állítja a szakembereket: a meglévő rendszer közel 600 éve szerves része a könyvelés világának, és egy merőben új rendszer implementálása rengeteg időt, pénzt és energiát igényelne. Költségek közt nem csak a hardver és szoftverinfrastruktúra kiépítése jelentene hatalmas vállalást, de a számviteli szakemberek továbbképzése, vagy a több éves implementálási projekt extra költségei.

Rendszerszintű technikai falakat jelent az interoperabilitás is. A blokklánc rendszerek által használt adatstruktúrák gyakran eltérnek egymástól, más protokollokkal, más konszenzus-

mechanizmusokkal dolgoznak, és nem átjárhatóak, egymással nem tudnak közvetlen kommunikálni, így elengedhetetlen mérföldkőként lebeg annak a megoldása, hogy az adatkonzisztencia fenttartása mellett, a különböző blokklánc rendszerek szinkronizálhatóak, átjárhatóak legyenek, azok egymással kommunikálni tudjanak.

Láthatjuk, hogy a rendszerrel nem véletlen foglalkoznak a fejlesztő és könyvelő cégek egyaránt, hisz alapjaiban változtatná meg a pénzügyi szektort, mind bizalom, mind hatékonysági téren. A rendszer technológiai és szabályozási kérdései ismertek, és mindkét szakma folyamatosan dolgozik a kérdések és kihívások tisztázásán, így a közeljövőben elérhetővé válhat egy merőben új könyvelési struktúra, ami a megbízhatóságon, átláthatóságon és biztonságon alapul.

A különböző szektorokban készített interjúk alapján, és a nemzetközi kutatások alapján a **hipotézisem megerősítést nyert.**

Bemutatásra került, hogy a blokklánc technológia felhasználásában rengeteg automatizációs lehetőség rejlik, amivel csökkenthetnénk az adminisztratív terhet a számviteli szakembereken, így gyorsabb és hatékonyabb munkavégzést eredményezne, míg a felszabaduló humán erőforrást pedig át lehetne csoportosítani emberi szemet igénylő feladatokhoz, ezzel javítva a könyvelések és értékelések minőségét.

Az automatizációnak és a felgyorsuló könyvelési mechanizmusoknak köszönhetően megközelíthetjük a valós idejű könyvelést, ami átláthatóbb főkönyveket és pénzügyi adatokat vonz maga után, hisz valós idejű pénzügyi adatok alapján tudnának döntést hozni a vállalatok.

A blokklánc technológia sajátosságainak ismertetésével pedig bebizonyosodott, hogy a különböző kriptográfiai módszerek megmásíthatatlan főkönyvet eredményeznének, így az üzleti bizalom növekedne, és gyökereiben változtatná meg a könyvvizsgálói szakmát.

## 8. IRODALOMJEGYZÉK

- Association of Certified Fraud Examiners. (2024). *Occupational Fraud 2024: A report to the nations*.
- Belluci, M., Bianchi, D. C., & Manetti, G. (2022). Blockchain in accounting practice. *Meditari Accountancy Research*, 121-146.
- Bitcoin Transactions per Day*. (2024. október 07). Forrás: YCharts: [https://ycharts.com/indicators/bitcoin\\_transactions\\_per\\_day](https://ycharts.com/indicators/bitcoin_transactions_per_day)
- Fazzini, M., Fici, L., Montrone, A., & Terzani, S. (2016). A Modern Look At The Banco De' Medici: Governance And Accountability Systems In Europe's First Bank Group. *International Business & Economics Research Journal*, 272.
- Hughes, E. (1993. Március 9). *Cypherpunk's Manifesto*. Forrás: Activism: Cypherpunks: <https://www.activism.net/cypherpunk/manifesto.html>
- Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts., (old.: 839-858).
- Ototea, A. (1974). *A reneszánsz és a reformáció*. Budapest: Gondolat Kiadó.
- Robson, K. (1992). Accounting numbers as "Inscription": Action at a distance and the development of accounting. *Accounting, Organizations and Society*, 685-708.
- Sergeenkov, A. (2024. 10 17). *Ethereum's Surge Roadmap Targets 100,000+ Transactions Per Second*. Forrás: Forbes: <https://www.forbes.com/sites/digital-assets/2024/10/17/ethereums-surge-roadmap-targets-100000-transactions-per-second/>
- Stein Smith, S. (2018). Implications of Next Step Blockchain Applicationsfor Accounting and Legal Practitioners: A CaseStudy. *Australasian Accounting, Business and Finance Journal*, 77-90.
- Yuji, I. (1989). Momentum accounting and triple-entry bookkeeping: exploring the dynamic structure of accounting measurements. *Studies in Accounting Research*.
- Zéman, Z. (2021). Fókuszban a változás, avagy nemzetközi trendek a pénzügyi és számviteli oktatásban és kutatásban. *Budapesti Corvinus Egyetem* (old.: 50-60). Budapest: 2021.