Blokklánc létrehozása az egyetemi adatok tárolására és a fizetős egyetemi tananyagok automatikus kifizetése intelligens szerződés alkalmazásával

Bálint Krisztián

Egyetemi adjunktus, Óbudai Egyetem Keleti Károly Gazdasági Kar,
balint.krisztian1@uni-obuda.hu

Absztrakt A blokklánc technológia alkalmazása lehetőséget ad az egyetemeknek saját blokklánc létrehozására. Az oktatásban alkalmazott bolognai program újragondolásával a jövőben az egyetemek még szorosabban együtt fognak működni a közös tantervfejlesztés területén. Megállapítható, hogy különböző egyetemeken ugyanazokat a tárgyakat tanítják, ebből kifolyólag az egyetemi oktatókra még nagyobb terhek hárulnak, hiszen minden egyetemen a tananyagok feltöltésével, testreszabásával is foglalkozniuk kell. A kutatás célja egy olyan blokklánc létrehozása a gyakorlatban, illetve annak részletes bemutatása, ahová az egyetemi oktatók egységesen elkészített tananyagokat tölthetnek fel a jövőben. Hosszú távon minden bizonnyal számos előnnyel jár az egységes és általánosan elfogadott egyetemi blokkláncben tárolt tanterv. Ha az egyetem fizetős tananyagot is szeretne feltölteni a blokkláncba, akkor okosszerződést kell alkalmaznia. Az okosszerződés segítségével automatizáltan lehet a tananyagok kifizetését lebonyolítani, ez által terheket lehetne levenni az egyetemek válláról. Mivel a blokkláncban a blokkok szorosan egymásra épülnek, ezért a bennük tárolt oktatási tananyagokkal nehéz módosítani. Mivel az egyetemeknek naprakész tudást kell biztosítaniuk a hallgatóknak a tananyagoknak is naprakésznek kell lenniük. A tananyagok meghatározott időközönkénti módosítását a Soft-Fork blokklánc eljárással lehetett megoldani.

Kulcsszavak: Egyetemi tananyag, Okos szerződés, Soft-Fork

Bevezető

A blokklánc technológia ma még újdonságnak számít, holott naponta jelennek meg új ötletek ezen a területen. Az informatikusok még mindig ismerkednek a blokklánc alapú megoldásokkal és igyekeznek kihasználni a benne rejlő lehetőségeket.

A blokklánc technológia még nem terjedt el az egyetemi oktatásban, bár már számos területen sikeresen alkalmazzák, mint például:

- A blokkláncban tárolt egészségügyi feljegyzések lehetővé teszik a betegek számára, hogy strukturált adataikat elérhetővé váljanak az orvosok számára. Az ilyen típusú elektronikus beteg-egészségügyi nyilvántartások adatbázisai hamisításbiztossá tennék a bejegyzéseket, miközben lehetővé válna a betegek számára, hogy hozzáférjenek elektronikus egészségügyi nyilvántartásaikhoz (Radanović & Robert, 2018).
- Napjainkban sok bank és más pénzintézet is vizsgálja és alkalmazza a blokklánc alapú biztonsági rendszereket, amelyek csökkentik a kiberfenyegetések és csalások kockázatát. A NASDAQ nemrégiben bejelentette egy blokklánc-alapú digitális főkönyv bevezetésének tervét, amely lehetővé teszi a részvénykezelési képességeik fejlesztését (Demirkan et al, 2020).
- A világ a felhasználók és a gépek által generált digitális adatok mennyiségének és sokféleségének bővülésével néz szembe. A blokklánc technológia jelentős megoldásokat kínál a Big Data tárolásának, rendszerezésének és feldolgozásának megoldására (Karafiloski & Anastas, 2017).
- A zenészek okos szerződéseket köthetnek a kiadóval. Ennek előnye, hogy a decentralizált és teljesen átlátható szerződések megkötésével lehetőség nyílik azok határidőre történő kifizetésére, illetve siker esetén még magasabb jogdíjak megszerzésére is. Az okos szerződés alkalmazása által az előre meghatározott feltételeket külső befolyás nélkül valósítja meg. Végül, de nem utolsósorban, a Spotify 2017-ben megvásárolta a média blokkláncot (Perrera et al, 2020).

Az adatok biztonságos tárolása és elérése érdekében a tananyagok egységesen feltölthetők a blokkláncba. A blokklánc technológia alkalmazásával szabványosíthatók az oktatási anyagok, így az oktatóknak nem kell azokat újra és újra feldolgozniuk minden egyetemen. Amennyiben a hallgató egyetemet váltana, akkor a tananyag az egységesség következtében ugyanaz lenne, mint a többi egyetemen, így az oktatás még hatékonyabbá válna. A bolognai program fontos része, hogy az egyetemi tananyagk hasonlóak, így amikor a hallgató egyetemet vált, a hallgató a már felvett tárgyakat magával tudja vinni, így nem kell azokat újra levizsgáznia. A blokklánc technológia alkalmazása által az egyetemi tananyagok ellenőrzésére nincs szükség, hiszen a tananyag minden esetben egységes. Előfordulhat, hogy egyes kurzusok tananyagai fizetősek, ilyenkor okosszerződéssel érhetők el az egyetemi blokklánc tananyagai. Az okosszerződés segítségével a tananyag automatikusan, emberi beavatkozás nélkül elérhető és megvásárolható.

A kutatás a következő struktúra szerint épül fel:

- Decentralizált On-Chain és Off-Chain megoldások vizsgálata egyetemi adattárolás céljából UEDSC blokklánc létrehozása által,
- Egyetemi blokklánc létrehozása,
- Egyetemi tananyagok értékesítése okos szerződéssel,
- Soft-Fork végrehajtása az UDSC blokkláncon.

1 Elérhető blokklánc típusok vizsgálata az egyetemi tananyagok tárolása szempontjából

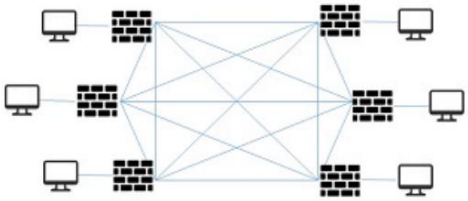
A decentralizált adattárolási megoldás használatával az adatok biztonságosabbak, mint a felhő alapú tárolás esetén, mivel több csomópont között vannak elosztva. Ezenkívül a tárolórendszerek nyilvános kulcsú titkosítást használnak. Az adatok rugalmasan osztódnak el a csomópontok között, és az intelligens szerződések is automatikusan felhasználásra kerülnek végrehajtás céljából (Jiang et al, 2020). A decentralizált adattárolás előnyei:

- A teljesítmény kiegyensúlyozott, mivel a csomópontok arányosan osztják szét az adatmennyiséget,
- A legtöbb hub a nap 24 órájában elérhető. Ha egyes csomópontok elérhetetlenné válnak, a többiek továbbra is kiszolgálják a felhasználót.
- Magas fokú függetlenség. Minden csomópont önállóan felelős a szabályok betartásáért, így megalkotva a blokklánc ökoszisztémát. Külső személy vagy hatóság nem korlátozza, és annak működését nem szabályozza.
- A felhasználók adatait feldarabolják, majd titkosítva továbbítják a csomópontoknak. DDoS támadás esetén így a rendszer működőképes marad.
- Ha egyes csomópontok nem működnek, vagy támadás esetén elérhetetlenné válnak, a többi csomópont megszakítás nélkül tovább működhet. A központosított rendszerben a központi szerver leállása esetén nagy valószínűséggel az egész rendszer működésképtelenné válik, így az adatok elérhetetlenné válnak (Amer, 2020).

A decentralizált blokklánc alapú adattárolásnak két fő megvalósítása létezik. Ezek az Off-Chain és On-Chain blokklánc megoldások.

Az Off-Chain nem tárol minden egyes adatot csomópontonként, ehelyett rögzíti azok hash értékét. Az adatok tényleges tárolása az egyetem merevlemezén történne. Ezeket az adatokat a mentés előtt több másolatra tördeljük (Alex, 2016).

Az On-Chain a legbiztonságosabb blokklánc alapú adattárolási megoldás, mivel minden adatot minden blokkban elment. Emiatt a hálózat működése lelassulhat, túlterhelés miatt elérhetetlenné válhat. Ezenkívül a csomópontok minden adatot megőriznek, és folyamatosan szinkronizálva vannak egymással. Ha támadás történik, az adatok nem vesznek el. Ez egy drága, de biztonságos megoldás (Bálint, 2021). Az alábbi első ábra a privát blokklánc felépítését mutatja.



1. ábra: Privát blokklánc
Forrás: Iuon-Chang, 2017

Mielőtt létrehozom saját, egyetemi adatok tárolására alkalmas blokkláncomat, megvizsgálom, milyen kész blokklánc alapú adattárolási megoldások állnak rendelkezésre, amelyek alkalmasak lehetnek egyetemi adatok tárolására. Ezek a következők:

- File Coin and
- IPFS (InterPlanetary File System).

A File Coin más decentralizált szolgáltatásokhoz hasonlóan a következő hátrányokkal rendelkezik:

- Magas volatilitás, ezért jelentős bizonytalanság övezi,
- Nehezen méretezhető,
- Sok esetben lassabbak, mint központosított társaik. A sebesség erősen adatbányászfüggő (Gábor & Kiss, 2018).

Az IPFS célja, hogy minden számítógépes rendszert ugyanahhoz a fájlrendszerhez kapcsoljon. Peer-to-Peer alapon működik. Előnye, hogy nincs központi szerver, és az adatokat a világ különböző pontjain tárolják.

Más rendszerekhez képest nagy teljesítményű blokktárolási modellt kínál, amelyben a tartalom és a cél hivatkozások találhatók. Ezenkívül a DHT (Distributed Hash Tables) megoldásokat önhitelesítő névterekkel kombinálja. Előnye, hogy az IPFS-csomópontoknak nem kell megbízniuk egymásban, így

csökken a meghibásodás lehetősége. Egyetlen hátránya, hogy nem nyújt erős adatvédelmi és kriptográfiai megoldást (Wang & Zhang, 2018).

Az IPFS és File Coin adattárolási megoldások áttekintése után arra a következtetésre jutottam, hogy az elérhető legmagasabb adatbázis-biztonság érdekében létrehozom saját egyetemi blokkláncomat, ahol személyesen tudom szabályozni az adatokhoz való hozzáférési jogokat. Az On-Chain blokklánc gyors és hatékony működése érdekében a blokkméretet 1 MB-ra maximalizálom.

2 Egyetemi blokklánc létrehozása

Önellátó, kari alapú blokklánc létrehozása esetén az oktatási intézmény saját maga határozhatja meg az adattárolás előnyös és kényelmes feltételeit. Ezek a következők lehetnek:

- Szélesebb hozzáférés a blokklánchoz,
- A blokkok méretének meghatározása,
- A használati feltételek meghatározása,
- Az eredeti blokk (genezis blokk), amelyhez az összes többi blokk csatlakozni fog, a kar tulajdonában marad,
- A blokklánchoz való hozzáférés korlátozása (csak az arra jogosultak használhatják),
- Az adatvédelmi politika meghatározása,
- A blokklánc több szerveren is elindítható a biztonság fenntartása érdekében,
- A csomópontok könnyebben felügyelhetők,
- A rendszer átláthatóbbá válik,
- Az esetleges adatkompromittálás könnyebben azonosítható (Bálint, 2021; Bálint, 2022).

Az UDSC (University Data Storage Chain) nevű egyetemi blokklánc létrehozásakor az első lépés a genezis blokk létrehozása. A genezis blokk létrehozása a második ábrán látható.

```
{
   "config": { // the config block defines the settings for our custom chain and has certain attributes to create a private blockchain
      "chainId": 987, // identifies UDSC blockchain
}
      "homesteadBlock": 0, // Homestead version was released with a few backward-incompatible protocol changes, and therefore requires a hard fork. UDSC chain however won't be hard-forking for these changes, so leave as 0
      "eip155Block": 0, // Homestead version was released with a few backward-incompatible protocol changes, and therefore requires a hard fork. UDSC chain however won't be hard-forking for these changes, so leave as 0
      "eip158Block": 0
   },
   "difficulty": "0x400", // This value is used to control the Block generation time of a Blockchain. The higher the difficulty, the statistically more calculations a Miner must perform to discover a valid block
   "gasLimit": "0x8000000",
   "alloc": {}}
}
```

2. ábra: Genezis blokk létrehozása
Forrás: Bálint, 2020

A kari alapú blokklánc a harmadik létrehozásának fontosabb lépéseit az alábbi ábrán figyelhető meg.

University chain-util generate UDSC
the default settings would be used:
/default ~ university chain/UDSC/chainsettings.dat
chainsettings.dat include:
Database addresses [receiver (cloud storage) IP address, sender (university) IP address],
Database system addresses [receiver (university database) IP address, sender IP address],
Terms of GDPR database.
Next, the UDSC blockchain would be initialized, and the genesis block would be created
universitychain UDSC
The server will be started in those few seconds after the genesis block has been found, then the node address needs to be connected:
UDSC@192.168.0.1:8008
After these steps, the connection can be attempted from a second server:
universitychain UDSC@192.168.0.1:8008
After the message confirming the chain has been initialized, permission is not given for connection to the database. The address would be copied and pasted: 192.168.0.2
finally, permission for connection would be granted:
universitychain UDSC grant 192.168.0.2 connect.

3. ábra: UDSC nevű blokklánc létrehozása
Forrás: Bálint, 2021; Bálint, 2022

3 Egyetemi tananyag kifizetése intelligens szerződés alkalmazásával

Az intelligens szerződés egy olyan digitális szerződés, amely a felhasználó digitális eszközeit szabályozza, megfogalmazza a résztvevő jogait és kötelezettségeit, amelyet a számítógépes rendszer automatikusan végrehajt [9].

Az intelligens szerződés a blokklánc technológián alapuló megoldás, amely automatikusan végrehajtja az abban meghatározott feltételeket egy külső harmadik fél, mint végrehajtó megkerülésével. Kizárólag a szerződési feltételekben előre meghatározott utasításokat hajtja végre. Ezeket a feltételeket triggereknek nevezzük. Az okosszerződés megkötéséhez a következő 4 feltétel szükséges:

- A szerződés tárgya,
- A feltételek pontos meghatározása. A szerződésben foglaltak csak akkor hajthatók végre, ha azok teljesülnek,
- A szerződés tárgyát és feltételeit digitális aláírással kell hitelesíteni,
- Utolsó lépésként egy blokkláncra is szükség van, ahol létre lehet hozni a szerződést (Budai, 2018).

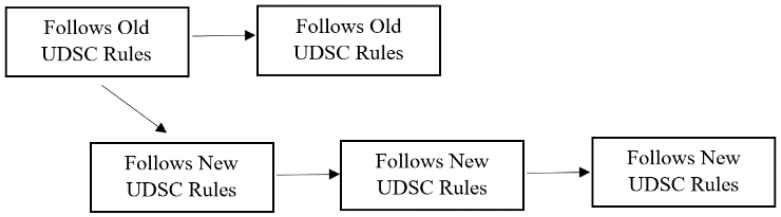
Az egyetemi UDSC blokklánc létrehozása után a tananyagok a megfelelő felhasználónév és jelszó megadása után válnak elérhetővé a hallgatók számára. Egyes tanfolyamok részeként azonban az órák fizetőssé válhatnak. Ez különösen jellemző az online oktatásra. Ha fizetős tartalom kerül fel a blokkláncra, akkor értelemszerűen csak fizetés után érhető el. Ebben nagy segítség az okos szerződés. Intelligens szerződés alkalmazásával a blokkláncban tárolt fizetős tananyagok elérhetővé válnak a hallgatók számára, miután kifizették azokat. Az alábbi negyedik ábra az intelligens szerződés alapú fizetési módot mutatja be.

```
1 contract University study material {
2 uint public price ;
3 uint public university's stock ;
4 /.../
5 function updatePrice ( uint _price ){
6 if ( msg. student == university )
7 price = _price ;
8 }
9 function buy ( uint quant ) returns ( uint ){
10 if ( msg. value < quant * price || quant > stock )
11 throw ;
12 stock -= quant ;
13 /.
```

4. ábra: Egyetemi tananyagok értékesítése okos szerződés alkalmazásával

4 Egyetemi tananyagok értékesítése okos szerződés által

Ha az oktatók a meglévő blokkláncba feltöltött tananyagot szeretnék a blokkláncban módosítani, akkor az egyetemi UDSC blokkláncon Soft-Fork-ot kell végrehajtani a blokklánc további folyamatos és zavartalan működése érdekében. Ez azt jelenti, hogy a Soft Fork rendszer akkor lép működésbe, amikor a rendszer új verzióhoz vagy új megállapodáshoz érkezik, és nem kompatibilis az előző verzióval, így az új csomópontok nem tudtak megegyezni a régi csomópontokkal. Mivel az új csomópontok számítási teljesítménye nagyobb súllyal bír, mint a régi csomópontok, a régi csomópontok soha nem hagyják jóvá az új csomópontokat, ennek ellennére az új csomópontok és a régi csomópontok továbbra is ugyanazon a láncon fognak működni. Létezik a kompatibilis láncok koncepciója is, amelyek akkor jönnek létre, amikor az új csomópontok és a régi csomópontok megegyeznek a konszenzusban, és az új csomópontok is csatlakozhatnak a régi csomópontokhoz (Memon et al 2018). Az ötödik ábra az UDSC blokklánc Soft-Fork-ját prezentálja.



5. ábra: Soft-Fork az UDSC blokkláncon
Forrás: Tehakerian, 2019

5 UDSC Blokklánc Összekapcsolása más Egyetemi Blokklánccal

Ahhoz, hogy összekapcsolhassunk egy blokkláncot egy másik blokklánccal, szükségünk van egy blokklánc-hídra. Általában a blokkláncok különálló zárt rendszerek, amelyek saját ökoszisztémával rendelkeznek. Ha az egyetemi UDSC blokkláncot össze akarjuk kötni egy másik blokklánccal, akkor blokklánc hidat kell használni. Ez a gyakorlatban azt jelentené, hogy ha a többi egyetemnek is megvan a saját blokkllánca, akkor létrejöhetne közöttük az átjárhatóság és a szorosabb együttműködés. A decentralizált híd esetében a fő cél az, hogy ne legyen szükség külső félre, aki csalni tud. Ebből kifolyólag szükség van egy okos

szerződésre és egy decentralizált hálózatra, illetve olyan érvényesítőkre, akik odafigyelnek a szabályok betartására.

A Polkadot blokklánc a blokklánc híd használata mellett az UDSC blokklánc összekapcsolására is használható más egyetemi blokkláncokkal, mivel a Polkadot célja, hogy keretet hozzon létre azon blokkok között, amelyek közös kapcsolatot kívánnak létrehozni. A blokkláncok csatlakozhatnak a Polkadothoz, és így párhuzamosan működhetnek.

Konklúzió

Annak ellenére, hogy az egyetemek nyitottak az új megoldásokra és modern oktatási módszereket alkalmaznak, a blokklánc-technológiában rejlő lehetőségeket még nem használják ki teljes mértékben.

Egy egységes és általánosan elfogadott egyetemi blokklánc létrehozásával az egyetemek közötti együttműködés még szorosabbá válhat. Az egységes tananyagok blokkláncban való tárolása manapság előremutató megoldásnak tekinthető, amely jelenleg kihasználatlan.

Okosszerződés alkalmazásával akár a fizetős tartalom is elérhetővé válik a hallgatók számára. Mivel folyamatos tananyagfejlesztésre van szükség, a blokkláncban történő módosítás a Soft-Fork segítségével megoldható.

Az egyetemeknek célszerű lenne lehetőségüktől függően saját közös blokkláncot létrehozniuk, nem pedig kész adattárolásra alkalmas blokkláncot bérelniük, hiszen így szabadon szabályozhatnák a blokklánc működési feltételeit és annak jogosultságait.

Hivatkozások

[1] Amer R., (2020). Centralized vs Decentralized Storage, Redefining Storage Solutions with Blockchain, https://blockgeeks.com/guides/centralized-vs-decentralized-storage-redefining-storage-solutions-with-blockchain-tech/ (utolsó letöltés, megtekintés dátuma: 2024. május 5.)

[2] Alex S. (2016) Ethereum blog, How to build serverless applications, https://blog.ethereum.org/2016/07/12/build-server-less-applications-mist (utolsó letöltés, megtekintés dátuma: 2024. május 5.)

[3] Bálint K. (2021). The connection of a Blockchain with Students' Attendance Register based on Security Cameras, IEEE 19th International Symposium on Intelligent Systems and Informatics (SISY 2021), Subotica, Serbia, 191, pp. 67-70 (2021).

[4] Bálint K. (2021). Possibilities for the Utilization of an Automatized, Electronic Blockchain-based, Students' Attendance Register, using a

Universities' Modern Security Cameras, Acta Polytechnica Hungarica, Volume 18(2), pp. 127-145 (2021) DOI: 10.12700/APH.18.2.2021.2.7,

[5] Bálint K. (2022). Data Security Structure of a Students' Attendance Register Based on Security Cameras and Blockchain Technology, IEEE Joint 22nd International Symposium on Computational Intelligence and Informatics and 8th International Conference on Recent Achievements in Mechatronics, Automation, Computer Science and Robotics (CINTI-MACRo 2022) : ProceedingsBudapest, Magyarország 418, 6, pp. 185-189.

[6] Bálint K. (2020). Modern, Decentralized Blockchain-Based Solutions for Saving Video Footage, IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY 2020) Danvers (MA), Amerikai Egyesült Államok: IEEE,185, pp. 11-14.

[7] Budai G. (2018). Blockchain is the world of cryptocurrencies and smart contracts, Budapest University of Economics, Faculty of Economics, Zalaegerszeg.

[8] Demirkan S., Demirkan I., McKee A. (2020). Blockchain technology in the future of business cyber security and accounting, Journal of Management Analytics 7(2), pp. 189-208.

[9] Gábor T., Kiss D. Kiss. (2018). An introduction to the world of cryptocurrencies, Economy and Finance, 5(1)

[10] Iuon-Chang L., Tzu-Chun L. (2017). A survey of blockchain security issues and challenges, International Journal of Network Security, 19(5) pp. 653-659 (2017).

[11] Jiang P., Guo F., Liang K., Lai J., Wen Q. (2020). Searchain: Blockchain-based private keyword search in decentralized storage, Future Generation Computer Systems, 107, pp. 781-792.

[12] Karafiloski E., Anastas M. (2017). Blockchain solutions for big data challenges: A literature review, IEEE Eurocon 17th International Conference on Smart Technologies. IEEE, (2017).

[13] Perera S., Nanayakkara S., Rodrigo M., Senaratne S., Weinand R. (2020). Blockchain technology: Is it hype or real in the construction industry, Journal of industrial information integration, 17.

[14] Memon M., Bajwa U. A., Ikhlas A., Memon Y., Malani, M. (2018). Blockchain beyond Bitcoin: block maturity level consensus protocol. IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), pp. 1-5.

[15] Radanović I., Robert L. (2018). Opportunities for use of blockchain technology in medicine, Applied health economics and health policy 16, Springer, pp. 583-590.

[16] Tchakerian A. (2019). Research Project the Blockchain Revolution Prospects and limitations, Research Dissertation for Master 2 Grande Ecole Programme, Researchgate project.

[17] Wang S., Zhang Y. (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access, 6, 38437-38450.