Privát blokklánc létrehozása a vállalati ügyfelek és vásárlási szokásaik biztonságos adattárolása céljából

Bálint Krisztián

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

Absztrakt: Napjainkban a blokklánc technológia egyre inkább részét képezi az informatika Világának. 10 évvel ezelőtt még mindenki számára ismeretlen matemaikai algoritmuson alapuló megoldás egyre több területen bizonyítja létjogosultságát. A blokkok szorosan egymáshoz kapcsolódva alkotják a blokkláncot, így az a decentralizáltságából adódóan hatékonyabb adatvédelmet biztosít, mint a centralizált társaik. A privát blokklánc létrehozása által hatékoyan lehet szabályozni a blokklánchoz való hozzáférést, ez által jogosultság hiányában idegen a blokkláncban tárolt adatokhoz nem férhet hozzá. A kutatás célja, hogy egy olyan blokklánc kerüljön létrehozásra, amelyben érzékeny vállalati adatok biztonságosan tárolhatóak akár hosszútávon is. A vállalati ügyfelek adataira kiemelt figyelmet kell fordítani, amennyiben azok kompromitálódnak, úgy a válalat értékes ügyfeleket veszíthet el, úgy a jelenben, mint a jövőben. A kutatás további célja, hogy a lehető legmegfelelőbb konszenzus mechanizmus kerüljön alkalmazásra a blokklánc adatainak rögzítése során. Ennek a megoldásnak a lényege, hogy a vállalati adatok hitelesítése a blokkláncban a legoptimálisabb és a legbiztonságosabb legyen.

Kulcsszavak: blokklánc technológia, biztonságos vállalati adattárolás, decentralizáltság

1 Bevezetés

A blokklánc technológia alkalmazása által hatékonyan lehet növelni a vállalati adatbázisbiztonságot, amely nem utolsó sorban az ügyfelek elégedettségéhez vezet. A vásárlási szokások vállalat szintű nyilvántartása az ügyfelek hatékonyabb kiszolgálását és megtartását teszi lehetővé biztonságos körülények között. A fogyasztói szokások folyamatosan változnak, új szokások alakulnak ki az online térben korábban elképzelhetetlen földrajzi és egyéb akadályok leküzdésével (Csiszárik-Kocsir, 2021). A blokkláncban tárolt adatok lehetővé teszik, hogy a Világ barmelyik pontját a vállalati adatokhoz biztonságosan hozzá lehessen férni, mivel az adatok biztonságos tárolása kulcsfontosságú (Tick, 2021).

A blokklánc tecnhológiában rejlő lehetőségeket az élet számos területén alkalmazzák. Ezek a következők:

- Kutatások folynak az útlevelek blokkláncban való tárolás lehetőségeiről. Ez által nehezebbé vállna az illetéktelen személyek bejutása olyan országokba, ahova nem lenne jogosultságuk (Fahmy, 2018).
- A bankszámla nyitásakor a bankok személyi ellenőrzést végeznek. Egyes bankok azonban tesztelik a blokklánc technológia alkalmazásának lehetőségét a nem személyes azonosítás során, mivel a tulajdonosok a blokkban tárolt adatok ellenőrzésével igazolhatják személyes adataik helyességét (Shong, 2017).
- A digitális művészet részeként sok művész elveszti az irányítást eszközei felett, amikor illegálisan eladják vagy hamisítják azokat. A blokklánc technológiának köszönhetően az eredeti mű a tulajdonosa birtokában marad, így csak a hamis mű sokszorosítható, ami veszít értékéből (Karafiloski, 2017).

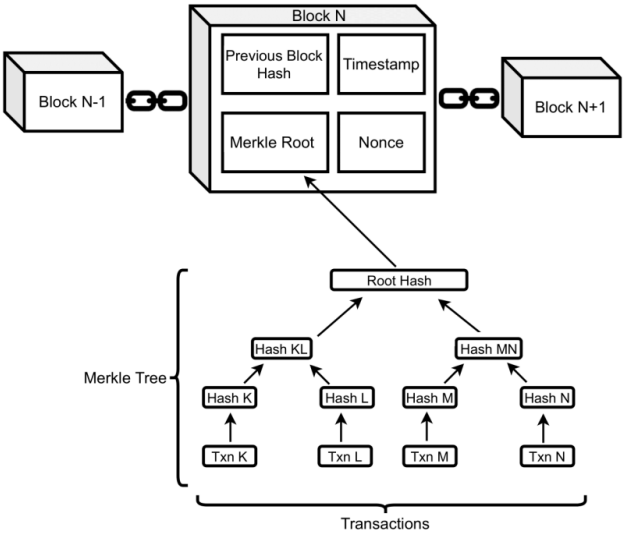
A kutatás a következő struktúra szerint épül fel:

- Vállalati blokklánc tulajdonságok vizsgálata,
- Konszenzus mechanizmus kiválasztása,
- Vállalati blokklánc létrehozása.

2 Vállalati blokklánc tulajdonságok

A vállati ügyfelek adatait célszerű egy privát blokkláncban tárolni. Minden blokklánc blokkok sorazatából épül fel. A blokkláncon belül a tényleges adattárolás a blokkokban történik, amely két részből áll:

- A fejlécből (amely a Hash értéket tárolja), valamint a
- Blokk törzséből (gyakorlatilag a törzsi részben tárolódnak el a vállalati adatok). Ennek részletes struktúráját az alábbi első ábra prezentálja.



1.ábra: Blokklánc felépítésének struktúrája
Forrás: Kushwala et al., 2022

Ahhoz, hogy egy blokklánc alkalmazható legyen vállalati adattárolás céljából, a következő fontos tulajdonságokkall kell, hogy rendelkezzen:

- Biztonság: Az aszimmetrikus titkosítás során két pár kulcs kerül használatra. A két pár kulcs matematikailag összefüggő nyilvános és egy privát kulcsból áll. A nyilvános kulcsot közzéteszik a rendszerben, viszont a privát kulcshoz, csak az arra jogosult felhasználó férhet hozzá és rendelkezhet vele.
- Pontosság: A blokklánc pontosságához és hibátlan működése érdekében a felhasználók szavazhatnak a rendszer fejlesztési irányvonalairól. Kizárólag a blokkláncban regisztrált felhasználók vehetnek ebben részt, amelyet az intézménynek folyamatosan ellenőriznie kell.
- Átláthatóság: A blokklánc az összes szavazólapot tárolja a rendszerben, így a felhasználók ellenőrizhetik, hogy hány szavazatot adtak le a jelöltek. Ez lehetővé teszi a rendszer egyszerű auditálását is.
- Autonómia: Ennek a szavazási rendszernek az egyik előnye, hogy decentralizált rendszer és mellőz mindennemű centralizált megoldást.
- Anonimitás: Az alkalmazott szavazási rendszer anonim. A blokkláncban tárolt adatok nem tartalmaznak információt a szavazókról, kizárólag a digitális pénztárcák nyilvános címét. A blokklánc rögzíti, hogy melyik pénztárca milyen tranzakciókat, illetve adatrögzítést bonyolított le, így a

felhasználók biztonságban érzik magukat, és nem kell aggódniuk a valódi személyazonosságuk felfedése miatt.

- Méltányosság: Minden blokklánc szavazó saját kívánsága szerint választhat és szavazhat.
- Hatékonyság: A rendszer feltételezhetően minimalizálja a műveletekhez használt költségeket, amely minden szempontból előnyös megoldás. (Christyono et al., 2021).

3 Konszenzus mechanizmus kiválasztása

A megfelelő konszenzus mechanizmus kiválasztása által a vállalati blokklánc biztonságát jelentősen növelni lehet, amely fontos részét képezi a kutatásnak, hiszen optimális adatbázisbiztonság nélkül érzékeny vállalati adatok kompromitálódhatnak. Saját értelmezés és megfogalmazás alapján a következő képpen definiálom az adatbázis-biztonságot:

Adatbázis-biztonság definíciója alatt a fenyegetettségeknek és a támadásokkal való ellenálást értjük, azokkal szemben alkalmazott védelmi erőforrások összeségét, amelyek megakadályozzák, hogy az arra jogosulatlan fizikai és jogi személyek, valamint kártékony számítógépes programok kihassanak azon működésére, bárminemű kárt okozzanak azok jogos tulajdonosainak, illetve felhasználóinak. Ide sorolandó még a bizalmasság, sértetlenség és rendelkezésre állás, valamint a letagadhatatlanság és a hitelesség biztonsági kritériumait is (Bálint, 2022).

3.1 Proof-of-Work (PoW) mechanizmus

A proof-of-Work megoldást egy úttörő konszenzusnak nevezik a blokklánc technológiában. A PoW számítás során az új blokkok egymással versenyeznek a létrehozásáért a számítási teljesítményük alapján. Ez a típusú algoritmus bányászati számítást igényel, amely során blokkokat állítanak elő. A PoW-ben adott a lehetőség az elágazásra, amelyet a hálózat használ a csomópontokon keresztül végzett matemaikai munka igazolása során (Bhutta, 2021).

3.2 Proof-of-Stake (PoS) mechanizmus

A PoS csökkentheti az egyes csomópontok bányászatának nehézségeit (Zhang, 2020), mivel a blokkok igazolására validátorokat alkalmaz a blokklánc. A PoS a PoW alternatívájaként jött létre, abból a célból, hogy csökkentse a blokklánc

üzemletetési költségeit. Vállalati szempontból ez mindenképpen előnyös megoldás.

A blokkgenerálási és tranzakció-visszaigazolási sebességet a PoW hálózatok viszonylag alacsony állandó sebességen tartják a biztonság érdekében, mivel a bányászok számos különböző blokkot javasolnak. Ezzel szemben a PoS mechanizmusok minden körében csak egy blokk készül, a blokkok generálása és a tranzakció megerősítése általában sokkal gyorsabb, így a PoS mechanizmus az utóbbi időben kezd egyre népszerűbbé válni (Nguyen, 2019).

Az első táblázat a PoW és a PoS konszenzus mechanizmus hasonlítja össze a legjellegzetesebb tulajdonságaik kiemelése mellett.

Proof of Work	**Proof of Stake**
A számítási kapacitást a bányászok határozzák meg.	Az új blokk hitelesítése a validátorok feladata.
A blokk létrehozásáért járó jutalmat az első bányász osztja szét a résztvevők között.	A jutalmat a validátorok kapják meg a hitelesítés során.
Magas számítási kapacitást igényel a blokklánc üemeltetése.	Energiahatékony megoldást alkalmaz.

1. táblázat: PoW és a PoS konsznezus mechanizmus összehasonlítása

3.3 Proof-of-Authority (PoA) mechanizmus

Azoknál a blokkláncoknál amelyeket vállalati, vagy banki felhasználásra szántak, az érdeklődő cégek alkotnak egy hálózatot a hardvereikkel. Ők ismerik egymást, közös a céljuk, motivációjuk és a részesedésük a tranzakciókból. Ez a permissioned blokklánc, általában három elv érvényesül a node-ok üzemeltetőinek kiválasztásában:

- Beazonosítás. Mivel a kezdeti validátorok is ismertek, elvárják egymástól, hogy minden új csatlakozóról tudni lehessen, hogy ki kicsoda.
- Korlátozott részvétel. A belépéshez feltétel a jó reputáció a színvonal tartása mellett, valamint az is, hogy legyen vesztenivalója annak, aki be szeretne szállni a validálásba. Ez lényegében a hírnév stakelése - aki technikai felkészültségben, vagy tisztességes együttműködésben lejáratja magát, az rontja a hírnevét a fintech iparban.
- Esélyegyenlőség. A fenti elbírálás minden résztvevőre ugyanúgy vonatkozik, ahogy az infrastruktúrát is azonos feltételek mentén üzemeltetik (Akela, 2022).

3.4 Konszenzus mechanizmus kiválasztása a vállalati blokklánc létrehozása előtt

A blokklánc esetében egy nem manipulálható, decentralizált technológia, azaz központi autoritás nélküli rendszerről beszélünk. A konszenzus algoritmusoknak (A Proof of Stake vagy Proof of Work) kell vállalniuk a feladatot, hogy megerősítsék a tranzakciókat és biztosítsák a hálózatba vetett bizalmat, amelyeket ez idáig egy központi szereplő (pl. bank) végzett.

Mindkét protokollnak vannak előnyei és hátrányai. A Proof of Work protokollnál a drága üzemeltetési költségek mellett fennáll az úgynevezett 51% -os támadás lehetősége. is Ez azt jelenti, hogy azok a Mining Pool-ok (bányászcsoportok), amelyek a bányászati teljesítmény legalább 51% -át maguknál központosítják, veszélyeztethetik a hálózat stabilitását és biztonságát. Ugyanakkor tucatszámra vannak bányászók az egész világon, akik ennek a protkollnak köszönhetően bányásznak, így létrehozva egy erős közösséget, ami hosszútávon garantálja a gazdasági stabilitást ezen a téren.

A Proof of Stake (PoS) protokollt sokkal könnyebben és olcsóbban lehet üzemeltetni, mint a Proof of Work-t. A (PoS) protokollnak is vannak még hiányosságai. Általában azokat a résztvevőket részesíti előnyben, akik az adott kriptovalutából nagy mennyiségben rendelkeznek. Például azok a befektetők, akik 10 000 dollárval rendelkeznek egy POS kriptovalutából, tízszer több blokkot érvényesíthetnek, mint azok a befektetők, akiknek ugyanabból a kriptovalutából csak 1000 dollára van. Ezenkívül egy bizonyos mennyiségű kriptovalutával kell rendelkezni a gazdasági megtérülés érdekében. Ezért egy minimális összeg alatti beruházás nem termel osztalékokat. Továbbá befektetőként érdemes szem előtt tartani, hogy még egy, a gyakorlatban nem annyira elterjedt protkollról van szó, ami befektetés szempontjából jelentős kockázattal is járhat (Germán, 2020).

Javaslatként fogalmazódik meg a vállalati szempontok figyelembe vétele mellett a Proof-of-Authority megoldás választása az blokkláncban tárolt adatok hitelesítésére és jóváhagyására.

3 Vállalati blokklánc létrehozása

A létrehozott vállalati blokklánc neve VB. Sokkal bonyolultabb privát hozzáférésű vállalati blokkláncot létrehozni, mint bérelni egy mások által létrehozott decentralizált tárhelyet. Amennyiben a vállalat a bérlés mellett teszi le a voksát, úgy annak el kell fogadnia a szolgáltató által megszabott feltételeket. Az önálló blokklánc esetében, a vállalat saját maga határozza meg a számára előnyős tárolási feltételeket.

Ezek a következőek:

- A vállalat szélesebb körű hozzáférést szerez a blokkláncho,
- Blokkok nagyságát meghatározhatja,
- A felhasználási feltételeket definiálhatja,
- A genezis-legelső blokk, amelyhez az összes többi blokk csatlakozni fog a vállalat tulajdonában marad,
- Blokklánc hozzáférését korlátozhatja (csak az erre jogosultak használhatják azt),
- Az adatvédelmi politikát meghatározhatja,
- A blokkláncot több szerveren is el tudja indítani a biztonság érdekében,
- A csomópontokat könnyebben felügyelheti,
- Az adattárolási rendszer és annak működése átláthatóbbá válik,

A vállalati blokklánc létrehozásának fontosabb lépését az alábbi harmadik ábra prezentálja.

Enterprise blockchain VB

the default settings would be used:

/default ~ university chain/VB/chainsettings.dat

chainsettings.dat include:

Database addresses [receiver (cloud storage) IP address, sender (company) IP address],

Database system addresses [receiver (company database) IP address, sender IP address],

Terms of GDPR database.
Next, the VB blockchain would be initialized, and the genesis block would be created

Enterprise blockchain VB

The server will be started in those few seconds after the genesis block has been found, then the node address needs to be connected:

VB@192.168.0.1:8008

After these steps, the connection can be attempted from a second server:

universitychain VB@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:

Enterprise blockchain VB grant 192.168.0.2 connect.

2. ábra: A VB nevű blokklánc forráskódjának fontosabb eleme

Összefoglalás

A blokklánc technológia alkalmazása vállalati szinten számos új lehetőséget nyújt, úgy az ügyfél adatok biztonságos tárolása területén, mint a vásárlási szokások nyomonkövetése szempontjából. Célszerű a vállalatoknak elgondolkodni azon a lehetőségen, hogy a saját és az ügyfeleik biztonságos adattárolása céljából egy privát hozzáférésű blokkláncot hozzanak létre. Ehhez mindössze egy informatikusra van szükség, aki jártas a blokklánctechnológiai gyakorlati megvalósításában. A kutatásban bemutatott blokklánc alkalmas akár az érzékeny adatok hosszútávú biztonságos tárolására is, mivel a centralizált adattárolás a múltban számos aggályt felvetett rendszergazda szinteken. A jövőben a decentralizált adattárolás hatékony alternatívája lehet a felhöben tárolt adatoknak, amelyen mindeképpen fontos elgondolkodni.

Hivatkozások

[1] Akela (2022). Mik ezek a konszenzus mechanizmusok? - Proof of Authority https://cryptofalka.hu/ismerteto/mik-ezek-a-konszenzus-mechanizmusok-proof-of-authority 2022. (utolsó letöltés, megtekintés dátuma: 2024. március 19.)

[2] 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) : Proceedings Budapest, Magyarország 418 p. pp. 185-189.

[3] Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., ... & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. Ieee Access, 9, pp. 61048-61073.

[4] Csiszárik-Kocsir Á, Garai-Fodor M. & János V. (2021). What has Become Important during the Pandemic? Reassessing Preferences and Purchasing Habits as an Aftermath of the Coronavirus Epidemic through the Eyes of Different Generations. Acta Polytechnica Hungarica, 18(11), pp. 49-74,

[5] Christyono, B. B. A., Widjaja, M., & Wicaksana, A. (2021). Go-Ethereum for electronic voting system using clique as proof-of-authority. Telkomnika (Telecommunication Computing Electronics and Control), 19(5), pp. 1565-1572.

[6] German, P. (2020). Mi is az a Proof of Stake és a Proof of Work? https://cryptofalka.hu/ismerteto/proof-of-work-proof-of-stake (utolsó letöltés, megtekintés dátuma: 2024. március 19.)

[7] Fahmy, S. F. (2018). Blockchain and its uses. Arab Academy for Science and Technology and Maritime Transport, Sheraton.

[8] Kushwaha, S. S., Joshi S, Singh, D., Kaur M. & Lee H. (2022). Systematic review of security vulnerabilities in ethereum blockchain smart contract". IEEE Access, 10, pp. 6605-6621.

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

[10] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T. & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE access, 7, pp. 85727-85745.

[11] Tick A. & Mai P. T. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), pp. 67-89.

[12] Shong, I. & Oh, J. (2017). A case study on business model innovations using Blockchain: focusing on financial institutions. Asia Pacific Journal of Innovation and Entrepreneurship, ISSN: 2398-7812.

[13] Zhang, R., & Chan, W. K. V. (2020). Evaluation of energy consumption in block-chains with proof of work and proof of stake. In Journal of Physics: Conference Series 1584(1), p. 012023. IOP Publishing.