



37. Országos Tudományos Diákköri Konferencia

Állam- és Jogtudományi Szekció

Budapest, 2025. március 24–26.

Rendező intézmény:

Károli Gáspár Református Egyetem

Állam- és Jogtudományi Kar



Állam- és Jog-
tudományi Szekció

**A jelent és a jövőt összekötő lánc: A blokklánc-technológia és az
adatvédelem összehangolása a GDPR tükrében**

Kézirat lezárásának dátuma:

2024/12/10

MI-használatra vonatkozó nyilatkozat

A dolgozat szerzőjeként kijelentem, hogy a dolgozat elkészítése során mesterséges intelligencia alapú eszközöket nem használtam. A kutatási folyamat során kizárólag az engedélyezett keresőmotorokat, elsősorban a Google keresési lehetőségeit vettem igénybe, melyeket a hiteles és releváns szakirodalmi források felkutatására, valamint a témához kapcsolódó információk gyűjtésére használtam. A dolgozat írásának minden fázisában csupán a Microsoft Word szoftver eredeti, beépített szövegszerkesztő funkcióira támaszkodtam, ideértve az alapvető szövegformázást, a helyesírás-ellenőrzést, valamint a szintaktikai és nyelvtani javításokat.

Nem vettem igénybe semmilyen külső gépi fordító, adatelemző, szövegalkotó vagy egyéb mesterséges intelligencián alapuló szolgáltatást. A dolgozat teljes tartalmának előállítását, a szöveg kidolgozását, valamint a kutatási eredmények értékelését kizárólag saját intellektuális teljesítményem eredménye, a fenti hagyományos eszközökkel kiegészítve. Célom az volt, hogy a tudományos munka során saját készségeimre és ismereteimre támaszkodva hozzak létre egy szakmailag hiteles és eredeti dolgozatot.

Tartalom

I. Bevezetés.....	4
II. A blokklánc hajnala és építőkövei	5
1. A blokklánc hajnala és története	5
2. A blokklánc építőkövei	7
III. Blockchain technológia és adatvédelmi kérdései	12
1. Az adatok megváltoztathatatlansága és az elfelejtéshez való jog problémája	12
2. Decentralizáció és az adattulajdonának kérdése a GDPR tükrében	16
3. A decentralizáció és a nemzeti szuverenitás viszonya	19
IV. Adatvédelem és blokklánc egyensúlya: hogyan lehet GDPR-barát a jövő?	21
1. Blockchain 2.0: új megoldások az adatvédelmi kihívások leküzdésére	22
2. De lege ferenda javaslatok	25
2.1. Álnevesítés és titkosítás adatvédelmi megoldása	25
2.2. A decentralizáció és a GDPR összehangolásának lehetséges módjai	28
V. Összegzés és következtetések	30
Szakirodalom	33
1. Könyvek, könyv fejezetek	33
2. Folyóiratok	33
3. Internetes hivatkozások	38
4. Jogszabályok, szabályzók	38

I. Bevezetés

A digitális technológiák gyors elterjedése mélyreható változásokat hozott a globális gazdaság működésében, átalakítva a vállalati rendszereket, a kormányzatok működését és az egyének közötti interakciókat. A modern társadalomban kulcsszerepet betöltő digitális gazdaság – amelyet a digitális platformok, elektronikus kommunikáció és adatvezérelt rendszerek jellemeznek – egy újfajta összekapcsoltságot és információáramlást valósított meg, ami az adatot mint gazdasági erőforrást az „új olajként” pozicionálja¹. Az adatok ilyen mértékű felértékelődése azonban kiterjedt adatvédelmi kihívásokkal jár, amelyek sürgetik a kiberbiztonsági intézkedések megerősítését és a felhasználói bizalom helyreállítását.

Az adatvédelem egyre fontosabb szerepét tükrözik az olyan szabályozások, mint az EU GDPR-ja vagy a kaliforniai CCPA, amelyek szigorúan meghatározzák az adatok gyűjtésére, tárolására és kezelésére vonatkozó előírásokat². Mindazonáltal a hagyományos, központosított adatkezelési rendszerek sérülékenysége egyre inkább láthatóvá válik a növekvő számú kibertámadások tükrében, amelyek alapjaiban kérdőjelezik meg ezen rendszerek alkalmazhatóságát egy globálisan összekapcsolt, elosztott gazdasági környezetben.

Egy ígéretes megoldásként tűnik fel a blokklánc-technológia, amely decentralizált struktúrájával és megváltoztathatatlanságával olyan biztonságos adatvédelmi keretet kínál, amely különösen vonzó az átláthatóságot és integritást igénylő iparágak számára³. A pénzügyi szektoron kívüli alkalmazása azonban korlátozott, ami a technológia mélyebb megértésének, valamint a meglévő szabályozásokhoz való integrációjának hiányából ered. A blokklánc tehát nemcsak technológiai újdonság, hanem potenciális kulcsfontosságú eszköz lehet a jövő digitális infrastruktúrájának kialakításában, amennyiben megfelelő szabályozási és technológiai környezet támogatja alkalmazását.

Éppen ezért ebben a dolgozatban arra vállalkozom, hogy megvizsgáljam, milyen szerepet tölthet be a blokklánc mint digitális infrastruktúra a szabályozási környezetben, feltárva a

¹ Raphael, Bömelburg., Oliver, Gassmann: Cambridge Analytica: Magical Rise, Disastrous Fall. In: Handbook of Digital Business Ecosystems. Zürich (Switzerland), Springer, 2021. pp. 387-396

² Isabella Corradini, Enrico Nardelli: Is Data Protection a Relevant Indicator for Measuring Corporate Reputation? In: Advances in Human Factors in Cybersecurity, 1st edition, London, Springer July 2020. pp. 135-140

³ Yukai Gao: Cyber Attacks and Defense: AI-Driven Approaches and Techniques. Academic Journal of Computing & Information Science, Vol. 7, Issue 7, 2024, pp. 41-46

technológia előnyeit és problémáit, és rámutatva arra, milyen jogi és technikai keretek biztosíthatják annak sikeres integrációját a digitális gazdaságban.

II. A blokklánc hajnala és építőkövei

1. A blokklánc hajnala és története

A blokklánc technológia fejlődése a 20. század végére nyúlik vissza, amikor az alapvető koncepciók már a Bitcoin megjelenése előtt is megfogalmazódtak. A blokkok kriptográfiailag biztosított láncának ötletét először Stuart Haber és W. Scott Stornetta kutatók vetették fel 1991-ben, amikor egy olyan rendszer kidolgozásán dolgoztak, amelyben a dokumentumok időbélyegzői nem manipulálhatók. E célból egy olyan módszert javasoltak, amely a dokumentumok sorozatának biztonságos tárolását tette lehetővé egy kriptográfiailag védett blokklánc segítségével⁴. Ez a megközelítés a modern blokklánc technológia korai előfutárának tekinthető, mivel elsődleges célja a digitális dokumentumok integritásának biztosítása, valamint azok visszadátumozásának vagy módosításának megakadályozása volt⁵.

Ezt a kezdeti elméleti munkát követően a decentralizált digitális valuta fogalma az 1990-es évek végén és a 2000-es évek elején kezdett kibontakozni. Különösen figyelemre méltó Wei Dai 1998-as javaslata a "b-pénz" névre keresztelt anonim, elosztott elektronikus pénzrendszerre, amely számos olyan alapvető elemet tartalmazott, amelyek később a blokklánc-technológia lényegévé váltak, mint például a decentralizált konszenzus és a munkavégzés bizonyítása (proof of work)⁶. Hasonlóan jelentős Hal Finney 2004-ben bemutatott "Reusable Proof of Work" (RPOW) rendszere, amely lehetővé tette a kriptográfiai tokenek felhasználók közötti átadását anélkül, hogy szükség lett volna egy központi hatóságra⁷. Bár ezek a korai kísérletek hozzájárultak a blokklánc technológia alapjainak lerakásához, még nem érték el azt a decentralizációs és biztonsági szintet, amely később a technológia lényegi részévé vált.

Az igazi áttörés 2008-ban következett be, amikor a rejtélyes Satoshi Nakamoto közzétette a "Bitcoin: A Peer-to-Peer Electronic Cash System" című tanulmányát. Ez a dokumentum egy decentralizált digitális valutarendszert, a Bitcoint javasolta, amely képes volt közvetítő harmadik fél nélkül működni. A Bitcoin központi eleme a blokklánc volt - a kriptográfiai elvek

⁴ Haber, S., & Stornetta, W. S. How to Time-Stamp a Digital Document. Journal of Cryptology, 1999, 3(2), 99-111.

⁵ Vora, G. Cryptocurrencies: Are Disruptive Financial Innovations Here? Modern Economy, 2015 July, 6(7), , pp. 816-831

⁶ Dai, W. b-money 1998, <http://www.weidai.com/bmoney.txt> (2024.08.16)

⁷ Finney, H. Reusable Proof of Work (RPOW). (2004) <https://nakamotoinstitute.org/finney/rpow/index.html> (2024.08.16)

és a decentralizált számítástechnika innovatív alkalmazása, amely lehetővé tette a tranzakciók biztonságos, átlátható és hamisításmentes rögzítését egy elosztott hálózaton keresztül⁸. A rendszer legnagyobb újítása abban rejlett, hogy képes volt megoldani a kettős költekezés problémáját egy olyan konszenzusmechanizmus alkalmazásával, amely biztosította, hogy minden tranzakciót csak egyszer rögzítsenek, így kiküszöbölve a központi hatóság szükségességét a tranzakciók hitelesítéséhez⁹.

Nakamoto blokklánc-konceptiója forradalmi jelentőséggel bírt, mivel több, már létező technológiát - kriptográfiai hash-funkciókat, Merkle döntési fákat és elosztott hálózatokat - integrált egy koherens és gyakorlati rendszerré¹⁰. Az első Bitcoin-tranzakcióra 2009 januárjában került sor, amely hivatalosan is elindította a blokklánc korszakát. Az ezt követő években a Bitcoin fokozatosan népszerűvé vált a kriptográfusok és technológusok szűkebb közösségében, miközben a szélesebb nyilvánosság számára továbbra is ismeretlen maradt¹¹.

A blokklánc technológia először a pénzügyi szektorban vált népszerűvé, ahol az intézmények gyorsan felismerték annak képességét a tranzakciók feldolgozásának, elszámolásának és rögzítésének alapvető átalakítására. Néhány vállalkozó hamar rájött, hogy a blokklánc alapelvei nem korlátozódnak csupán a digitális pénznemekre, hanem számos más területen is hasznosíthatók. 2013-ra a technológia széles körű figyelmet kapott, és ekkor jelentek meg az első altcoinok is, amelyek a Bitcoin blokkláncának módosított verzióival új funkciókat és fejlesztéseket kínáltak¹². A blokklánc fejlődésének egyik legfontosabb mérföldköve az Ethereum 2015-ös bevezetése volt Vitalik Buterin által, amely az okos szerződések bevezetésével új távlatokat nyitott a technológia számára, lehetővé téve programozható tranzakciók és decentralizált alkalmazások (DApps) létrehozását¹³.

Ez a felismerés és az altcoinok megjelenése indította el a blokklánc technológia dinamikus fejlődését. A pénzügyi szektorban elért kezdeti sikerek ösztönözték a fejlesztőket és

⁸ Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System 2008 <https://bitcoin.org/bitcoin.pdf> (2024.08.16)

⁹ Nicolas, Cachanosky. Can Bitcoin become money? The monetary rule problem. Australian Economic Papers, 2019, 58(4), 365-374.

¹⁰ Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Illustrated Edition). Princeton, New Jersey, Princeton University Press. 2016, pp336

¹¹ Walch, A. The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk. Journal of Risk Finance, 2015, 18(4), 837.

¹² Aksoylu, E. EXAMINING THE RELATIONSHIP BETWEEN BITCOIN AND ALTCOINS. PressAcademia Procedia, 2024,18(1), 92-94.

¹³ Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014 [https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum Whitepaper - Buterin 2014.pdf](https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum%20Whitepaper%20-%20Buterin%202014.pdf) (2024.08.17)

vállalkozókat, hogy a blokklánc alkalmazását más iparágakra is kiterjesszék. Ahogy a technológia egyre kiforrottabbá vált, különböző ágazatok kezdtek rájönni a blokkláncban rejlő potenciálra, ami széleskörű adaptációhoz vezetett, és új innovációk, valamint alkalmazások kifejlesztését eredményezte a digitális világ számos területén.

2. A blokklánc építőkövei

A blokklánc-technológia fejlődése a kezdeti koncepcióktól napjainkig tartó átalakulás során számos olyan innovációval gazdagodott, amelyek jelentősen bővítették a technológia alkalmazási lehetőségeit és kiterjedését. Eredetileg a Bitcoin alapjául szolgáló technológiaként fejlesztették ki, de mára messze túllépett az eredeti digitális pénzként való alkalmazásán. A blokklánc ma már egy sokoldalú és erőteljes platformként ismert, amely képes kezelni az adatkezelés és adatvédelem néhány legkritikusabb kihívását. A blokklánc kulcs attribútumai a decentralizáció, átláthatóság, megváltoztathatatlanság és az önvégrehajtó intelligens szerződések megjelenése együttesen járultak hozzá ehhez a fejlődéshez, és tették a blokkláncot a különböző iparágak digitális átalakulásának központi elemévé¹⁴. Ugyanezek a jellemzők jelentős potenciált rejtenek az adatvédelem megerősítésében is, aminek eredményeképpen a blokklánc egyre fontosabb eszközzé válik a személyes és érzékeny információk védelmében.

A decentralizáció a blokklánc-technológia egyik legfontosabb alapelve, amely az adatvédelem szempontjából is kulcsszerepet játszik. A hagyományos adatkezelési rendszerek gyakran központosított adatbázisokra támaszkodnak, ahol az adatokat egyetlen szervezet, például egy vállalat, önkormányzat, állami intézmény vagy pénzintézet tárolja és felügyeli¹⁵. Bár a központosítás egyszerűsítheti az adatkezelést és a hozzáférést, ugyanakkor jelentős biztonsági kockázatokat is magában hordoz. Egy központosított rendszer egyetlen hibapontot jelent; ha ez sérül – legyen szó kibertámadásról, hardverhibáról vagy belső fenyegetésről –, az összes adat veszélybe kerülhet, kitéve azt az adatbiztonsági incidensek, jogosulatlan hozzáférés vagy adatvesztés kockázatának¹⁶.

Ennek az a legfőbb oka, hogy a blokklánc technológiában az adatokat nem egyetlen központi szervezet vagy hatóság ellenőrzi, hanem egy decentralizált hálózat, ami a technológia egy

¹⁴ Casino, F., Dasaklis, T. K., & Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 2019 March 36, 55-81

¹⁵ Abdullah, N., Håkansson, A., & Moradian, E. Blockchain-based approach to enhance big data authentication in distributed environment. In *Proceedings of the International Conference on Ubiquitous and Future Networks (ICUFN)* 2017, pp. 887–892

¹⁶ Srinivasan, S. Privacy protection and data breaches. *Proceedings of Informing Science & IT Education Conference (InSITE)* 2015, 429-444.

építőköve, amely számos résztvevőből – úgynevezett csomópontokból – áll. Minden csomópont tárolja a hálózat teljes adatállományának egy másolatát, és részt vesz az adatok hitelesítésében és frissítésében¹⁷. Amikor valaki egy új tranzakciót vagy adatot szeretne hozzáadni a blokklánchoz, azt először a hálózat összes csomópontjának ellenőriznie kell. Ez az ellenőrzési folyamat egy konszenzusmechanizmusnak nevezett módszeren alapul. A konszenzusmechanizmus lényege, hogy a hálózat többségének – vagyis a csomópontok nagy részének – egyet kell értenie abban, hogy a hozzáadni kívánt adat vagy tranzakció helyes és jogos¹⁸. Ezáltal csak akkor kerül be az új adat a blokkláncba, ha a hálózat többsége jóváhagyja azt.

A konszenzusmechanizmusok különböző módokon működhetnek, attól függően, hogy milyen típusú blokkláncról van szó. Az egyik leggyakoribb ilyen mechanizmus a "proof of work" (munka bizonyítéka), amelyet például a Bitcoin hálózat is használ. Ebben a rendszerben a csomópontoknak bonyolult matematikai problémákat kell megoldaniuk ahhoz, hogy jóváhagyhassák a tranzakciókat. Az első csomópont, amelyik megoldja a problémát, hozzáadhatja az új adatot a blokkláncához, és jutalmat kap érte¹⁹. Ez a folyamat rengeteg időt és energiát igényel, ami lényegesen megnehezíti, hogy bárki manipulálja a rendszert. Egy másik ismert konszenzusmechanizmus a "proof of stake" (részesezés bizonyítéka), amelyben a csomópontok közötti döntéshozatal azon alapul, hogy kinek van több részesezése a hálózatban²⁰. Itt azok a csomópontok kapnak nagyobb beleszólást az új adatok jóváhagyásába, amelyek nagyobb részesezéssel rendelkeznek a hálózatban.

Ezek a mechanizmusok biztosítják, hogy a blokkláncban tárolt adatok csak akkor változhassanak, ha a hálózat résztvevőinek többsége egyetért a változtatással. Ezáltal a blokklánc rendszere biztonságos és ellenálló a manipulációval szemben, hiszen nem elég egyetlen csomópontot befolyásolni – a hálózat többségét kellene megtéveszteni, ami rendkívül nehéz és költséges feladat, ugyanis nem egy részt vevő hanem a hálózatban részt vevők többsége ellen kéne sikeres kibertámadást végrehajtani²¹. Ez a decentralizáció jelentősen javítja

¹⁷ Yi, Sun., Ying, Shao. Research on Data Security Communication Scheme of Heterogeneous Swarm Robotics System in Emergency Scenarios. *Sensors*, 2022 August, 22(16):6082-6082.

¹⁸ Abhi, A.I.; Shin, S.Y. BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. *IEEE Access* 2019, 7, 103231–103249

¹⁹ Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System 2008, <https://bitcoin.org/bitcoin.pdf> (2024.08.15)

²⁰ Ganesh, C., Orlandi, C., & Tschudi, D. Proof-of-Stake Protocols for Privacy-Aware Blockchains. *IACR Cryptology ePrint Archive*, 2018 January 2018 Vol, pp1105

²¹ Yang, Xiao., Ning, Zhang., Wenjing, Lou., Y., Thomas, Hou. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys and Tutorials*, 2020, 22(2), 1432-1465

az adatvédelmet, mivel csökkenti az adatbiztonsági incidensek valószínűségét, és biztosítja, hogy az adatok biztonságosak és ellenállóak maradjanak a potenciális fenyegetésekkel szemben. Például az egészségügy területén, ahol a betegadatok rendkívül érzékenyek, a blokklánc decentralizált modellje biztosítja, hogy egyetlen hibapont se veszélyeztesse a betegadatok biztonságát²².

A decentralizáció emellett a magánélet védelmét is erősíti, mivel az egyéneknek vagy szervezeteknek nem kell megbízniuk egy központi hatóságban az adataik kezelését. Ehelyett az irányítás elosztott módon történik, és az adatokat csak a hálózat résztvevői között osztják meg, a hozzáférést pedig kriptográfiai módszerekkel biztosítják²³. Ez a megközelítés különösen értékes lehet olyan szabályozási keretek között, mint a GDPR esetében, ahol a személyes adatok védelme és annak biztosítása, hogy az egyének ellenőrzést gyakorolhassanak saját adataik felett, elsődleges fontosságú.

Továbbá az átláthatóság a blokklánc egy másik alapvető tulajdonsága, amely szintén hozzájárul az adatok védelmének fokozásához. A hagyományos rendszerekben az adatkezelés gyakran zárt ajtók mögött történik, és korlátozott rálátást biztosít arra, hogy az adatokat hogyan kezelik, dolgozzák fel vagy éppen kik férnek hozzájuk. Az átláthatóság hiánya megnehezítheti az ellenőrzést, az elszámoltathatóságot és az adatvédelmi szabályok betartását²⁴. A blokklánc azonban egy nyilvános főkönyvi rendszerben működik, ahol minden tranzakció és adatcsere nyilvánosan rögzítésre kerül, és a hálózat minden résztvevője számára látható²⁵. Az átláthatóság ez a formája biztosítja, hogy az adatkezelés minden lépése teljes mértékben nyomon követhető és függetlenül ellenőrizhető legyen, így egyértelmű és ellenőrizhető nyilvántartás jön létre arról, hogyan kezelték az adatokat, ki és milyen körülmények között férhetett hozzájuk.

Az adatvédelem terén az átláthatóság alapvető fontosságú a bizalom kiépítése és a szabályozási előírások betartásának biztosítása szempontjából. Például a pénzügyi szektorban, ahol az átláthatóság elengedhetetlen a csalások megelőzése érdekében és a tisztességes gyakorlatok biztosításához, a blokklánc nyilvános főkönyve valós idejű betekintést nyújthat a szabályozóknak és az érdekelt feleknek a tranzakciókba, csökkentve ezzel a tiltott

²² Agbo, C. C., & Mahmoud, Q. H. (Blockchain in Healthcare: Opportunities, Challenges, and Possible Solutions. *International Journal of Healthcare Information Systems and Informatics*, 2020, 15(3), 54-71

²³ William, J., Gordon., William, J., Gordon., Christian, Catalini., Christian, Catalini. *Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.. Computational and structural biotechnology journal*, 2018, 16, 224-230.

²⁴ Gal, M. S., & Aviv, O. The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 2020, 16(3), 349-391.

²⁵ Wong, D. *Real-World Cryptography*. Shelter Island, New York, Manning Publications. 2021, 400 pages.

tevékenységek, például a pénzmosás kockázatát²⁶. Hasonlóképpen, az ellátási lánc irányításában az átláthatóság biztosítja, hogy minden szereplő - a gyártóktól a fogyasztókig - nyomon követheti a termékek eredetét és útját, ellenőrizve, hogy azok megfelelnek-e az etikai normáknak, és hogy nem történt-e velük visszaélés²⁷. Ez a szintű átláthatóság nemcsak az esetleges szabálysértések esetén való felelősségre vonás esélyét és gyorsaságát növeli, hanem lehetővé teszi a fogyasztók számára, hogy megalapozott döntéseket hozzanak, hiszen biztosak lehetnek abban, hogy az általuk vásárolt termékek a valódiak és az eladó vagy gyártó által állított etikus forrásból származnak.

A blokklánc-technológia immutabilitása, amely szorosan összefügg az átláthatósággal, hatékony adatvédelmi mechanizmusként funkcionál. A hagyományos adatkezelési rendszerekkel szemben, ahol az adatok gyakran módosíthatók vagy törölhetők – akár minden nyom nélkül is –, a blokklánc megváltoztathatatlansága biztosítja, hogy az egyszer rögzített adatok biztonságosan és változatlanul megmaradjanak, hacsak nem jön létre egy többségi konszenzus, amely kifejezetten jóváhagyja a változtatást²⁸. Ez a konszenzuson alapuló modell azt jelenti, hogy ha egy adat bejegyzésre került a blokkláncba, azt csak akkor lehet megváltoztatni vagy törölni, ha a hálózat résztvevőinek többsége ebben egyetért.

A blokklánc minden egyes blokkját kriptográfiai védelem óvja, és az egyes blokkok szorosan kapcsolódnak az előzőkhöz, létrehozva ezzel egy folytonos és rendkívül ellenálló nyilvántartási láncot²⁹. Bármilyen kísérlet egy blokk módosítására nemcsak az adott blokk megváltoztatását tenné szükségessé, hanem az összes azt követő blokk módosítását is, ami csak akkor lehetséges, ha a hálózat résztvevőinek többsége beleegyezik³⁰. Ez a megoldás gyakorlatilag lehetetlenné teszi az illetéktelen változtatásokat, mivel a szükséges konszenzus megszerzése rendkívül bonyolult és költséges lenne.

²⁶ Motunrayo, Oluremi, Ibiyemi., David, Olanrewaju, Olutimehin. Blockchain in supply chain accounting: Enhancing transparency and efficiency. Finance & accounting research journal, 2024, 6(6), 1124-1133

²⁷ Kumar, S. K. D., Nassa, V. K., Uike, D., Kalra, A., Sahu, A. K., Athavale, V. A., & Saravanan, V. A Comparative Analysis of Blockchain in Enhancing the Drug Traceability in Edible Foods Using Multiple Regression Analysis. Journal of Food Quality, 2022(1), 6 pages

²⁸ Xu, Z., Luo, X., Xue, K., Wei, D. S. L., & Li, R. SEREDACT: Secure and Efficient Redactable Blockchain with Verifiable Modification. In 43rd IEEE International Conference on Distributed Computing Systems, ICDCS 2023, Hong Kong, July 18-21, 2023 (pp. 818-828).

²⁹ Kaushik, S., & El Madhoun, N. Analysis of Blockchain Security: Classic Attacks, Cybercrime and Penetration Testing. In Proceedings of the Eighth International Conference On Mobile And Secure Services (MobiSecServ 2023), Miami, USA, 2023, pp. 1-6.

³⁰ Garman, C., Green, M., & Miers, I. . Accountable Privacy for Decentralized Anonymous Payments. In Proceedings of the International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Springer, 2017, pp. 81-98.

A feltételes megváltoztathatatlanság különös jelentőséggel bír azokban az ágazatokban, ahol az adatok integritása elengedhetetlenül fontos. Például a jog világában a blokklánc technológia alkalmazása lehetővé teszi szerződések, tulajdoni lapok és egyéb kritikus dokumentumok olyan nyilvántartásának létrehozását, amely gyakorlatilag hamisíthatatlan. A blokklánc megváltoztathatatlansága biztosítja, hogy ezek a dokumentumok csak akkor módosíthatók, ha a hálózat résztvevőinek többsége kifejezetten egyetért a változtatással. Ezáltal a blokklánc alapú nyilvántartások hosszú távon pontosak és megbízhatóak maradnak, ami biztonságos és hiteles alapot biztosít a jogi eljárások számára.

Az adatvédelem szempontjából a feltételes megváltoztathatatlanság lehetőséget nyújt a szervezetek számára, hogy megfeleljenek a szabályozási követelményeknek, amelyek előírják az adatok és tranzakciók pontos, változatlan nyilvántartását. Például a pénzügyi intézmények a blokklánc technológia alkalmazásával garantálhatják, hogy a tranzakciós nyilvántartások állandóak és megváltoztathatatlanok maradnak, hacsak a hálózat résztvevői többségi konszenzussal nem döntenek másként. Ez a technológiai megközelítés biztosítja a vitathatatlan ellenőrzési nyomvonalat, amely elengedhetetlen a jogszabályi megfelelés igazolásához³¹. A blokklánc tehát nemcsak a dokumentumok és tranzakciók integritását védi, hanem a jogi és pénzügyi ágazatokban a jogszabályi előírásoknak való megfelelést is támogatja, biztosítva a dokumentumok hitelességét és megbízhatóságát az idő múlásával.

A blokklánc-technológia fejlődését jelentős mértékben elősegítette az önvégrehajtó intelligens szerződések integrálása, melyek lehetővé teszik az összetett tranzakciók automatikus, biztonságos és hatékony lebonyolítását. Ezek az intelligens szerződések programozott feltételek mentén működve kiküszöbölik a közvetítők szükségességét, minimalizálják az emberi hibák kockázatát, és garantálják a szerződésekben rögzített előírások pontos betartását³².

Ez a megközelítés az adatvédelem területén is jelentős változást idézhet elő sőt akár paradigma változást is, hiszen segítségével az adatokhoz csak akkor és csak olyan módon férnek hozzá az arra jogosultak, ahogyan az a szerződésben meghatározott. Például a digitális identitások kezelésében az egyének maguk irányíthatják személyes adataik használatát, míg az

³¹ Sonawane, N., Gupta, P., Laksh, C., & Gururaja, H. S. A Blockchain Solution for Enhancing Risk Management and Transparency in Loan Disbursements. In Proceedings of the 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT), October 20, 2023, pp. 1-6.

³² Alharby, M., & van Moorsel, A. Blockchain Based Smart Contracts: A Systematic Mapping Study. In Proceedings of the 3rd International Conference on Artificial Intelligence and Soft Computing 2017 pp. 125-140

egészségügyben az intelligens szerződések a betegadatokhoz való hozzáférést a páciens által előre megadott hozzájárulásokhoz kötik.

A blokklánc e tulajdonságai nemcsak a jelenlegi adatkezelési és -védelmi gyakorlatok átalakítását teszik lehetővé, hanem új alapokra helyezhetik a bizalom, az átláthatóság és a hatékonyság elveit is. Ahogy a technológia egyre szervezettebben épül be a digitális infrastruktúrába, várhatóan megoldást nyújt olyan jövőbeli kihívásokra is, amelyek ma még csak körvonalazódnak. Így a blokklánc a digitális gazdaság egyik kulcsfontosságú pillérévé válhat, ösztönözve az iparági innovációt, és megteremtve az átláthatóbb, biztonságosabb és megbízhatóbb digitális ökoszisztéma alapjait.

III. Blockchain technológia és adatvédelmi kérdései

1. Az adatok megváltoztathatatlansága és az elfelejtéshez való jog problémája

A blokklánc-technológia egyik legismertebb és legnagyobbra értékelt tulajdonsága a megváltoztathatatlanság, amely azonban jelentős kihívást jelent az Európai Unió által bevezetett GDPR "elfelejtéshez való jogával" kapcsolatban. A blokklánc lényegét egy decentralizált főkönyv adja, amelyben a rögzített adatok nem módosíthatók, nem törölhetők. Ez a megváltoztathatatlanság alapvetően hozzájárul az adatok integritásának, biztonságának és megbízhatóságának biztosításához, mivel a blokkláncon tárolt bármely tranzakció vagy adat időrendben és megmásíthatatlanul rögzített, ezáltal hamisíthatatlan³³. Azonban ez a jellemző éles ellentétben áll a GDPR 17. cikkében meghatározott "elfeledtetéshez való joggal", amely biztosítja az egyének számára a személyes adataik törléséhez való jogot.

A GDPR 17. cikke értelmében az érintettek jogosultak kérni személyes adataik törlését, amennyiben azok már nem szükségesek az eredeti célokhoz, amelyek érdekében gyűjtötték őket, ha visszavonják az adatkezeléshez adott hozzájárulásukat, vagy ha az adatok jogellenesen kerültek feldolgozásra³⁴. E rendelkezés célja, hogy az egyének számára teljes ellenőrzést biztosítson személyes adataik felett, összhangban az adatvédelem és a magánélet védelmének

³³ Смирнов, А. В. Прозрачность и децентрализация в блокчейне: технические и социальные аспекты. Журнал цифровых технологий и систем, 2022(3), 50-62.

³⁴ European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.(Továbbiakban GDPR) Section 3, Article 17 1.) a.)-d.)

szélesebb körű céljaival³⁵. A blokklánc-technológia kontextusában azonban az adatok állandósága és megváltoztathatatlansága súlyos jogi és technikai dilemmákat vet fel.

A legfőbb probléma abból fakad, hogy a blokklánc struktúrája alapvetően nem teszi lehetővé az adatok egyszerű törlését. Még ha egy adat rekord titkosítva van, vagy hozzáférhetetlenné is válik, az eredeti adat továbbra is a blokkláncon marad, ami sérti a GDPR teljes körű törlésre vonatkozó követelményeit³⁶. Ezt a problémát tovább súlyosbítja a blokklánc decentralizált jellege, ahol nincs egyetlen központi hatóság, amely felhatalmazással bírna az adatok eltávolítására a hálózatról. Ez a decentralizált struktúra különösen megnehezíti az adattörlési kérelmeknek való megfelelést.

A fenti kihívásokra válaszul különböző technikai megoldásokat javasoltak a blokklánc megváltoztathatatlanságának és a GDPR által biztosított elfeledéshez való jog összeegyeztetésére. Az egyik lehetséges megközelítés a láncon kívüli tárolás (off-chain storage) alkalmazása, amely során a személyes adatokat a blokkláncon kívül, hagyományos adatbázisokban tárolják, és a blokkláncon csupán az adatok hash értéke vagy hivatkozása található³⁷. Törlési kérelem esetén a láncon kívüli adatok törölhetők, így a blokkláncon tárolt hash érték jelentéktelenné válik az eredeti adatok nélkül³⁸. Bár ez a megoldás lehetőséget kínál a GDPR-nak való megfelelésre, bevezeti a központosított adattárolás hagyományos kockázatait, és aláássa a blokklánc decentralizált természetét.

Egy másik lehetséges megoldás a kriptográfiai törlés (cryptographic erasure), amely során a személyes adatokat titkosítják, mielőtt azokat a blokkláncon tárolnák. A titkosítási kulcsokat az érintett vagy egy megbízható harmadik fél birtokolja. Amennyiben az érintett a személyes adatai törlését kéri, a titkosítási kulcsok megsemmisíthetők, így az adatok a blokkláncon gyakorlatilag hozzáférhetetlenné válnak³⁹. Bár ez a módszer megőrzi a blokklánc megváltoztathatatlanságát azáltal, hogy az adatokat sértetlenül megtartja, egyúttal gyakorlatilag

³⁵ Kasper, Gabriel. *People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts*. 1. Auflage, Dike Verlag in Kooperation mit Nomos Verlag, Reihe: Recht der neuen Technologien (RnT), 2021, Band 2 pp 450

³⁶ Bolesch, Lara/Mitschele, Andreas: *Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie*, Kreditwesen 2016, 1125-1129

³⁷ Sharma, Dhramandra, and Monika Saxena. "Different Cryptographic Hash Functions for Security in the Blockchain." 2023 International Conference on Data Science and Network Security (ICDSNS), July 2023, pp. 1-6

³⁸ Muharrem, Tuncay, Gencoglu. *Mathematical Analysis of The Hash Functions as a Cryptographic Tools for Blockchain*. Firat University Turkish journal of science & technology, 2022 17(2):187-201

³⁹ Salih, Hatim. "Quantum Erasure Cryptography." *Frontiers in Physics*, vol. 4, Optics and Photonics, 20 May 2016

"törli" azokat, mivel azok visszakereshetelenné válnak⁴⁰. Azonban a GDPR értelmében a kriptográfiai törlés jogi megfelelése továbbra is vitatott, hiszen az adatok technikailag még mindig léteznek a blokkláncon, bár nem hozzáférhető formában.

Ezen túlmenően az adatvédelmet fokozó technológiák, mint például a zéró-tudásbizonylatok (zero-knowledge proofs) vagy a szelektív közzétételi protokollok, ígéretes lehetőségeket kínálnak a blokklánc és a GDPR közötti összhang megteremtésére. Ezek a technológiák lehetővé teszik, hogy bizonyos adatokra vonatkozó igazolások szülessenek anélkül, hogy a mögöttes adatokat ténylegesen felfednék, ezáltal rugalmasabb adatkezelést biztosítva a blokklánc-hálózatokon belül⁴¹. Noha ezek a megoldások ígéretesek, még viszonylag korai fejlesztési fázisban vannak⁴², és további kutatásokra, valamint jogi validálásra van szükség ahhoz, hogy teljes mértékben megfeleljenek a GDPR előírásainak, és széles körben alkalmazhatók legyenek a gyakorlatban

A blokklánc-technológia megváltoztathatatlansága és a GDPR "elfeledtetéshez való jog" közötti feszültség számos gyakorlati példán keresztül világosan megmutatkozik, amelyek rávilágítanak a technológia és a jogi keretek közötti alapvető ellentmondásokra. Az Európai Unió Blokklánc Megfigyelőközpontja és Fóruma (European Union Blockchain Observatory and Forum, továbbiakban: EUBOF) által vizsgált esetek jól demonstrálják ezeket a konfliktusokat.

A blokklánc-alapú földhivatali rendszerrel kapcsolatos svédországi ügy jelentős példája a blokklánc-technológia megváltoztathatatlansága és a GDPR követelményei, különösen a 17. cikk szerinti „elfeledtetéshez való jog” közötti konfliktusnak. A svéd földhivatali projekt célja az volt, hogy a blokklánc technológia megváltoztathatatlan jellegének kihasználásával növelje az ingatlanügyletek átláthatóságát és biztonságát⁴³. Végeredmények azt tüzték ki, hogy

⁴⁰ Liu, Chen, Hoda Aghaei Khouzani, and Chengmo Yang. "ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives." 2017, vol. 1, pp. 132–148.

⁴¹ Kobelt, Max, Michael Sober, and Stefan Schulte. "A Benchmark for Different Implementations of Zero-Knowledge Proof Systems." 2023 IEEE International Conference on Blockchain (Blockchain), December 2023 pp33-40

⁴² Tyagi, Shobha. "A Review on Zero Knowledge Proof Vulnerabilities in Zcash." 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICIT), November 2023, pp. 872-877

⁴³ Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay, and Kairos Future. The Land Registry in the Blockchain. July 2016. https://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf (2024.09.01)

hamisíthatatlan nyilvántartást hozzanak létre a tranzakciókról, ezáltal növelve a bizalmat és a hatékonyságot az ingatlanpiacon⁴⁴.

Amikor azonban egy, a projektben részt vevő földtulajdonos kérte személyes adatainak törlését, a blokklánc megváltoztathatatlan szerkezete jelentős jogi kihívást jelentett. A blokkláncra egyszer már rögzített adatokat nem lehetett megváltoztatni vagy eltávolítani, mivel a rendszer decentralizált jellege miatt egyetlen hatóság sem tudta módosítani a nyilvántartásokat⁴⁵. Az, hogy a földtulajdonos kérésének nem lehetett eleget tenni, alapvető ellentmondásra világított rá a blokklánc felépítése és a GDPR jogi kerete között, amely bizonyos feltételek mellett előírja a személyes adatok kérésre történő törlését.

Ez az eset jogi vitát váltott ki, hangsúlyozva a blokklánc-technológia meglévő adatvédelmi jogszabályokba való integrálásának kihívásait. A svéd eset kiemeli, hogy további jogi és technikai innovációra van szükség ahhoz, hogy a blokklánc előnyeit össze lehessen egyeztetni a GDPR-hoz hasonló adatvédelmi előírások által támasztott szigorú követelményeivel.

Egy másik példát a Steemit platform szolgáltatott, amely egy blokklánc-alapú közösségi hálózat. A Steemit lehetővé tette a felhasználók számára, hogy tartalmaikat és interakcióikat a Steemit blokkláncán rögzítsék, ami biztosította a tartalom hitelességét és megmásíthatatlanságát. Azonban amikor néhány felhasználó élni kívánt a GDPR szerinti "elfeledtetéshez való jogával", és kérte a személyes adataik és tartalmaik törlését, a platform nem tudta teljesíteni ezeket a kéréseket⁴⁶. Mivel a Steem blokklánc megváltoztathatatlan szerkezetű, a rögzített adatok nem voltak eltávolíthatók vagy módosíthatók. Ez a helyzet jelentős jogi problémákat vetett fel, mivel a platform nem tudott megfelelni a GDPR adatvédelmi előírásainak.

Ezek a konkrét példák egyértelműen rávilágítanak arra, hogy a blokklánc-technológia megváltoztathatatlansága és a GDPR által biztosított adatvédelmi jogok összehangolása jelentős kihívások elé állítja a jogi és technológiai közösségeket. A probléma lényege abban rejlik, hogy a blokklánc decentralizált és módosíthatatlan struktúrája alapvetően ellentétes azzal a jogi követelménnyel, amely az érintettek számára lehetővé teszi személyes adataik törlését. Az ilyen esetek nemcsak a technológiai rendszer és a jogi normák közötti összeütközést

⁴⁴ Jasmontaite, Lina, and Eleni Kosta. "GDPR Compliance in Blockchain Technology: A Closer Look at the Swedish Land Registry Case." *European Data Protection Law Review*, vol. 5, no. 3, 2019, pp. 324-337.

⁴⁵ Godyn, Mateusz, Michal Kedziora, Yingying Ren, Yongxin Liu, and Houbing Herbert Song. "Analysis of Solutions for a Blockchain Compliance with GDPR." *2022 September Scientific Reports*, vol. 12, no. 1: 15021

⁴⁶ Shen, Charlie. "Blockchain Immutability: A Double-Edged Sword in Compliance with GDPR's Right to Erasure." *Journal of Technology Law & Policy*, vol. 22, no. 1, 2019, pp. 45-67

demonstrálják, hanem rávilágítanak arra is, hogy a jogalkotás és a technológiai innováció fejlődése nem minden esetben képes szinkronban haladni.

Felmerül tehát a kérdés, vajon érdemes-e tovább keresni a megoldásokat a blokklánc-technológia és a GDPR által előírt „elfeledtetéshez való jog” összhangjának megteremtésére, vagy el kell engedni ezt a technológiát, mert a vele járó kockázatok, veszélyek és kihívások felülmúlják a potenciális előnyöket. Az egyik oldalról nézve a blokklánc számos iparági folyamatban fokozott adatbiztonságot, átláthatóságot és megbízhatóságot ígér, elősegítve a bizalomépítést és az innovációt⁴⁷. Viszont ha egy másik szemszögből nézzük ezt a technológiát a jelenlegi szabályozási elvárások, különösen a GDPR adatvédelmi szempontjai mellett csupán nagy nehézségek árán lehet alkalmazni, kérdésessé válik, hogy a rendszer nem rejt-e több veszélyt, mint amennyi hasznot hoz. Ebben a kontextusban a hálózat alapvető módosíthatatlansága, a központosított hatalom hiánya, illetve a személyes adatok kezelésének nehézségei nem csupán technikai vagy jogi akadályok, hanem potenciális kockázati tényezők is, amelyek nyomán mérlegelendő, hogy a blokklánc hosszú távon alkalmas eszköz-e egy olyan világban, ahol az adatvédelem és az egyéni jogok tiszteletben tartása kiemelt fontosságú.

2. Decentralizáció és az adattulajdonának kérdése a GDPR tükrében

A blokklánc technológia megjelenése jelentősen megzavarta az adatok tulajdonjogának és ellenőrzésének hagyományos fogalmait, különösen az Európai Unió általános adatvédelmi rendeletének (GDPR) szabályozási környezetében. A hagyományos központosított adatkezelési rendszerekben az adatgyűjtést, -feldolgozást és -tárolást jellemzően egy egyedi szervezet irányítja - legyen az egy vállalat, kormányzati szerv vagy szolgáltató⁴⁸. Ez a központosított modell egyértelmű felelősségi hierarchiát hoz létre: az adatgyűjtést végző szervezetet a GDPR rendelkezései szerint „adatkezelőnek” nevezik ki, és ezáltal felelősséggel tartozik azért, hogy a személyes adatok feldolgozása a szabályozási előírásoknak szigorúan megfelelően történjen. A GDPR 4. cikkének (7) bekezdése szerint „adatkezelő” az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő

⁴⁷ Rademacher, Thomas. "Die DSGVO und Blockchain-Technologien: Herausforderungen und Lösungsansätze im europäischen Datenschutzrecht." Zeitschrift für europäisches Privatrecht, 2021, vol. 30, no. 1, , pp. 58-75

⁴⁸ Hohmann, Balázs. "Provisions of the DSA and DMA Regulations Affecting Consumer Contractual Relations concerning Digital Goods and Services." In Medias Res, 2023/2, pp. 69-91.

kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja⁴⁹.

A blokklánc technológia azonban alapvetően más előfeltételek alapján működik, amelyeket a decentralizáció és az elosztott főkönyvi mechanizmusok jellemeznek. Egy ilyen decentralizált blokklánc-hálózatban az adatokat csomópontok sokasága terjeszti, amelyek mindegyike a blokklánc főkönyvének teljes vagy részleges másolatát tartja fenn⁵⁰. Ez az elosztott topológia összetett kérdéseket vet fel az adatok tulajdonjogával és ellenőrzésével kapcsolatban. Amikor a személyes adatok számos független csomóponton keresztül replikálódnak, a GDPR értelmében adatkezelőnek minősülő szervezet azonosítása óriási kihívássá válik. A blokklánc decentralizált ethosza megnehezíti az ellenőrzés és a felelősség egyszerű kijelölését, mivel az adatokat a hálózat valamennyi résztvevője közösen kezeli és hitelesíti⁵¹. Az ellenőrzésnek ez a számtalan független szereplő közötti szétszóródása nem illeszkedik zökkenőmentesen a GDPR hagyományos modelljéhez, amely egy egyértelműen azonosítható, az adatvédelmi megfelelésért felelős szervezet meglétét feltételezi.

Ezt az összetettséget tovább fokozza a blokklánc-hálózatokban gyakran előforduló pseudo anonimitás. A blokkláncon belüli tranzakciók átláthatóak és minden résztvevő számára láthatóak, ugyanakkor az érintett személyek vagy szervezetek személyazonossága jellemzően rejtjelezett címek vagy álnevek mögé rejtőzik. A GDPR értelmében a személyes adatok közé tartozik minden olyan információ, amely egy azonosított vagy azonosítható természetes személyre vonatkozik⁵², ami azt jelenti, hogy még az álneves adatok is a rendelet hatálya alá tartozhatnak, ha az egyén további adatpontok segítségével újra azonosítható. A blokklánc kontextusában ez sarkalatos kérdéseket vet fel azzal kapcsolatban, hogy az álneves adatokat feldolgozó vagy tároló hálózati résztvevők adatkezelőknek vagy adatfeldolgozóknak tekintendők-e, és hogy a GDPR értelmében ugyanolyan szabályozási kötelezettségek vonatkoznak-e rájuk, mint a hagyományos központosított szervezetekre.

A decentralizált rendszerekben az adatok tulajdonjogát és ellenőrzését övező kétértelműség jelentős jogi fejtörést okoz, amikor a GDPR-nak való megfelelés biztosítására törekszünk. A rendelet előírja, hogy az adatkezelők és adatfeldolgozók megfelelő technikai és szervezeti

⁴⁹ GDPR I Fejezet 4 cikk 7. bek.

⁵⁰ Rademacher, Thomas. "Die DSGVO und Blockchain-Technologien: Herausforderungen und Lösungsansätze im europäischen Datenschutzrecht." Zeitschrift für europäisches Privatrecht, vol. 30, no. 1, 2021, pp. 58-75.

⁵¹ Kühling, Jürgen, and Martini, Mario. "Blockchain und die Datenschutz-Grundverordnung: Die Konfrontation zwischen Technik und Datenschutzrecht." Juristenzeitung (JZ), vol. 74, no. 5, 2022, pp. 239-247.

⁵² GDPR I Fejezet 4 cikk 1. bek

intézkedéseket hajtsanak végre a személyes adatok védelme érdekében⁵³, és hogy haladéktalanul válaszoljanak az érintettek személyes adataikhoz való hozzáférésre, azok helyesbítésére és törlésére vonatkozó kéréseire⁵⁴. Egy decentralizált blokklánc-környezetben alapvető megfelelési kihívássá válik annak meghatározása, hogy ki a felelős e kötelezettségek teljesítéséért. A felelősség kijelölésére szolgáló hagyományos mechanizmusok nem alkalmasak egy olyan környezetben, ahol az ellenőrzés egy decentralizált hálózaton belül oszlik el, ahol nincs központi irányító személy.

Ezen problémák miatt elengedhetetlen egy olyan jogi keret kidolgozása vagy módosítása, amely képes ezen ökoszisztémák sajátosságait befogadni, ugyanakkor biztosítja a GDPR szellemiségével összhangban álló adatvédelmet. Ennek egyik lehetséges módja az adatkezelők és adatfeldolgozók szerepeinek újragondolása. Egy nyilvános blokklánc esetében elméletileg minden csomópont közös adatkezelővé válhat a GDPR 26. cikkének értelmében, amely előírja, hogy a közös adatkezelőknek egyértelmű megállapodásban kell rögzíteniük az érintett jogainak gyakorlására és az információk rendelkezésre bocsátására vonatkozó felelősségük megoszlását⁵⁵.

Ezzel a modellalapú megközelítéssel minden hálózati résztvevő közösen vállalná a GDPR-ral való megfelelésért viselt felelősséget. Ez magában foglalná az érintettek kérésére való válaszadást és a megfelelő adatvédelmi intézkedések végrehajtását. A közös adatkezelési modell azonban gyakorlati akadályokkal szembesül: a blokklánc-hálózatok gyakran több ezer csomópontból állnak, amelyek különböző joghatóságok alatt működhetnek, így a GDPR-megfelelés koordinációja jelentősen bonyolulttá válik⁵⁶.

Ezen túlmenően, minden egyes csomópont üzemeltetőjének felelősségre vonása az adatkezelői kötelezettségek betartásáért újabb kihívásokat vet fel, különösen, ha sok csomópont álnéven vagy névtelenül működik⁵⁷. Az adminisztratív terhek és a jogi komplexitás kezelése érdekében egyértelmű szabályozási iránymutatások és speciális adatvédelmi megállapodások kialakítása válik szükségessé, amelyek biztosítják a GDPR megfelelés elérését a blokklánc decentralizált környezetben.

⁵³ Шишкин, А.А. "Блокчейн и GDPR: проблемы защиты данных и перспективы регулирования." *Право и экономика*, 2020, № 6, стр. 78-86.

⁵⁴ GDPR III Fejezet 15-17 cikk

⁵⁵ GDPR IV Fejezet 1. Szakasz 26.cikk 1.bek

⁵⁶ Härting, Niko, and von Maltzan, Philipp. "Blockchain und die DSGVO: Lösungsansätze für das Recht auf Vergessenwerden." *Computer und Recht*, vol. 35, no. 3, 2022, pp. 129-136.

⁵⁷ Berberich, Manuel, and Steiner, Malgorzata. "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?" *European Data Protection Law Review*, vol. 2, no. 3, 2016, pp. 422-426.

Evvel a blokklánc-technológia alapjaiban alakította át az adatkezelés hagyományos struktúráit, új kihívásokat teremtve a GDPR szempontjából. A decentralizált ökoszisztémákban az adatkezelői és adatfeldolgozói szerepek újragondolása kulcsfontosságú annak érdekében, hogy az adatvédelmi kötelezettségek teljesítése átlátható és fenntartható legyen. A GDPR 26. cikke által kínált közös adatkezelési modell elméleti alapot biztosíthat arra, hogy minden csomópont részt vállaljon a szabályozási megfelelésben, azonban a külön joghatóságok és a névtelen működés kihívásai miatt ennek gyakorlati megvalósítása összetett feladat.

3. A decentralizáció és a nemzeti szuverenitás viszonya

A blokklánc-technológia decentralizált, határokon átívelő természete ma már nem csupán elméleti aggály, hanem kézzelfogható fenyegetést jelent a nemzeti szuverenitásra, amelynek középpontjában a magyar állam adatvédelmi és információkezelési képességei állnak. A globálisan elosztott hálózatok és a földrajzi határokon átívelő adatáramlás okánál fogva az államok által alkalmazott hagyományos eszközök – a jogalkotás, a hatósági ellenőrzés, a szankciók alkalmazása – nehezebben, lassabban és korlátozott hatékonysággal érvényesíthetők⁵⁸. Ha a magyar nemzetállam nem cselekszik időben és hatékonyan, a decentralizáció a magyar digitális tér feletti szuverén befolyás fokozatos, visszafordíthatatlan gyengülését eredményezheti. Ennek következtében Magyarország, mint önálló, saját szabályokat meghatározni képes állam, akár elveszítheti is a kontrollt a területén zajló adatkezelési folyamatok felett, ami a nemzeti érdekképviselő súlyos csorbulásához vezet.

A legsürgetőbb feladat e fenyegetés elhárítása érdekében a belső jogalkotási kapacitások és a szabályozási keretek megerősítése. A magyar államnak szigorúbb, egyértelműbb és átfogóbb jogszabályokat kell alkotnia az adatvédelemmel és a blockchain-alapú megoldásokkal kapcsolatban, amelyek nem csupán deklaratív jellegűek, hanem ténylegesen kikényszeríthetők. A hazai normák pontosan körvonalazhatják a külföldi szolgáltatók piaci belépésének feltételeit, előírhatják a magyar állampolgárok adatait kezelő rendszerek regisztrációs és ellenőrzési kötelezettségeit, rögzíthetik a felelősség megosztását, valamint a technológiai compliance kritériumait. Ezzel párhuzamosan a már működő Szuverenitásvédelmi Hivatal hatáskörének gyakorlati alkalmazására, a hatósági ellenőrzések és szankciók megerősítésére is szükség van, hogy a hazai jogszabályok ne csupán papíron, hanem a gyakorlatban is megvédjék a magyar érdekeket.

⁵⁸ Kelemen Roland, Farkas Ádám: A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. In *Medias Res*, 2022/1. pp 96–108.

A határozott belső jogalkotási és hatósági fellépés kulcsfontosságú, mert az európai uniós szabályozás, mint például a GDPR, ugyan minimális adatvédelmi sztenderdeket nyújt, de önmagában nem garantálja a magyar szuverenitás megőrzését egy olyan technológiával szemben, amely eredendően a határokon átvéelő decentralizációra épül⁵⁹. Más országok, mint például Kína, a „kiberszuverenitás” elvét hangsúlyozva elismerik az állam jogát arra, hogy saját határain belül meghatározza az internet és a digitális technológiák működésének szabályait⁶⁰. Ez az elméleti kiindulópont ugyanakkor a globális, határtalan adatáramlás valóságában csak egy úton védhető meg, mégpedig ha a belső jogalkotás valóban erős, következetes és betartható szabályrendszert hoz létre. Az internetszuverenitás elve tehát ebben az esetben akkor válhat érdemi eszközzé és gondolattá, ha a nemzeti jogalkotó képes lépést tartani a technológiai fejlődéssel, és hatékonyan akadályozza meg, hogy a blockchain-rendszerek az állami kontroll kikerülésével működjenek.

Emellett elengedhetetlen a proaktív diplomáciai és nemzetközi érdekérvényesítési stratégia. Magyarországnak a regionális és globális szintén is képviselnie kell saját álláspontját, és olyan megállapodások, ajánlások létrejöttét szorgalmaznia, amelyek tiszteletben tartják a nemzeti szabályozási mozgásteret. Ha a hazai szabályozás erős alapokon nyugszik, a nemzetközi normák alakítása során a magyar fél magabiztosabban érvényesítheti érdekeit⁶¹. Evvel a lépéssel elkerülhető, hogy a nemzetközi standardok túlzott ráhatása vagy az engedékeny szabályozás a magyar érdekek háttérbe szorulását eredményezze.

A tét tehát rendkívül magas: a belső jogalkotás megerősítése és a hatósági kontroll szigorítása nélkül a nemzeti szuverenitás elvesztése reális forgatókönyvvé válhat. A technológia globális, határokat átlépő jellege pedig tovább súlyosbítja a helyzetet, hiszen a hazai előírások betartatása állandó küzdelmet jelent a nemzetközi szereplőkkel szemben. Magyarországnak minden rendelkezésére álló eszközt – a jogszabályalkotástól a diplomácia eszköztárá és az intézményi kapacitásfejlesztésen át a nemzetközi együttműködésekig – mozgósítania kell annak érdekében, hogy megőrizze önrendelkezését a digitális korszakban. Csak így érhető el, hogy a blockchain-technológia ne aláássa, hanem a nemzeti érdekeket is figyelembe vevő rendben működjön, biztosítva a magyar állampolgárok adatainak szuverén védelmét, a magyar társadalmi és

⁵⁹ Namrata, Singh., Shallu, Bishnoi, Navigating GDPR Compliance: The Intersection of Data Governance, Accountability, and Organizational Culture. International journal of innovative research in engineering & multidisciplinary physical sciences, 2024, 12(4) pp1-7

⁶⁰ Gosztanyi Gergely, "Kiber Gulág" és 'Digitális Vasfüggöny', avagy az Internetszuverenitás kérdései Oroszországban." *Iustum Aequum Salutare*, 2024 Vol. XX, No. 3, pp. 17–29.

⁶¹ Zsolt Zódi, A legal theory of platform law, PRO PUBLICO BONO – Public Administration, 2024/1, 101–125

kulturális értékek tiszteletben tartását, valamint a nemzetgazdaság megerősítését a hálózatos és globalizálódó digitális térben.

IV. Adatvédelem és blokklánc egyensúlya: hogyan lehet GDPR-barát a jövő?

Az előző fejezetek elemzése rávilágított arra, hogy a blokklánc-technológia és az Európai Unió általános adatvédelmi rendelete (GDPR) közötti összeegyeztethetőség kérdése nem csupán elméleti kihívás, hanem a gyakorlatban is sürgető problémát jelent. A blokklánc decentralizált, megváltoztathatatlan és átlátható jellege alapvetően új perspektívákat nyit az adatkezelés és -védelem területén, ugyanakkor alapvető konfliktusban áll a GDPR által előírt adatvédelmi követelményekkel. A megváltoztathatatlanság és a decentralizáció, amelyek a blokklánc legfontosabb erényei közé tartoznak, jelentős jogi dilemmákat vetnek fel, különösen az "elfeledéshez való jog" és az adatkezelői felelősség tekintetében⁶².

A digitális gazdaság fejlődésével és az adatok egyre növekvő jelentőségével párhuzamosan a magánélet védelme és az adatbiztonság iránti igény is fokozódik. A blokklánc-technológia ígéretes megoldásokat kínálhat ezen a területen, azonban a meglévő jogi keretek és a technológia sajátosságai közötti ellentmondások megnehezítik a technológia széles körű alkalmazását. Az érintettek jogainak védelme és a technológiai innováció előmozdítása közötti egyensúly megteremtése ezért kulcsfontosságú feladattá vált a jogalkotók, a szabályozó hatóságok és a technológiai szakemberek számára.

A feszültségek feloldása és a blokklánc-technológia GDPR-ral való összeegyeztetése érdekében elengedhetetlen a lehetséges megoldások átfogó vizsgálata. Ezen megoldásoknak figyelembe kell venniük a technológia egyedi jellemzőit, miközben biztosítják az adatvédelmi előírások betartását⁶³. A következő fejezetekben ezért arra összpontosítunk, hogy feltárjuk azokat az innovatív technológiai fejlesztéseket és jogi alkalmazkodásokat, amelyek hozzájárulhatnak e cél eléréséhez.

Elsőként a technológiai megoldások kerülnek górcső alá, amelyek között szerepelnek az adatvédelmet erősítő technológiák, mint például a zero-knowledge proof (zéró-tudás bizonyítékok) és a szelektív közzétételi protokollok⁶⁴. Ezek a fejlett kriptográfiai módszerek

⁶² Casino, Fran, Dasaklis, Thomas K., and Patsakis, Constantinos. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." *Telematics and Informatics*, vol. 36, March 2019, pp. 55-81.

⁶³ Lee, Jiho, and Kim, Jae. "Exploring Sidechains for Secure and Compliant Data Management in Financial Services." *International Journal of Finance and Economics*, vol. 26, no. 4, 2021, pp. 4212-4225.

⁶⁴ Bunz, Benedikt, et al. "Bulletproofs: Short Proofs for Confidential Transactions and More." *IEEE Symposium on Security and Privacy*, 2018, pp. 315-334,

lehetővé tehetik az adatok biztonságos és magánéletet tiszteletben tartó kezelését a blokkláncon belül, anélkül hogy sértenék annak megváltoztathatatlanágát és átláthatóságát. Emellett az olyan megközelítések, mint a láncon kívüli megoldások és sidechain-ek alkalmazása⁶⁵, szintén potenciális utat kínálnak a személyes adatok hatékony kezelésére és a GDPR követelményeinek való megfelelésre.

Másodsorban a jogi és szabályozási adaptációk szükségességét vizsgáljuk, amelyek során a meglévő jogi kereteket kellene módosítani vagy kiegészíteni a blokklánc egyedi tulajdonságainak figyelembevételével. A nemzetközi együttműködés és a jogharmonizáció kulcsfontosságú lehet annak érdekében, hogy a különböző joghatóságok egységesen kezeljék az új technológiák által felvetett adatvédelmi kihívásokat⁶⁶. Felmerül a lehetősége új jogi kategóriák bevezetésének is, mint például a "hálózati résztvevők" vagy a "decentralizált adatkezelők", amelyek jogilag jobban illeszkednének a blokklánc decentralizált struktúrájához.

Az előttünk álló elemzés célja tehát az, hogy átfogó képet nyújtson a lehetséges megoldásokról, és útmutatást adjon arra vonatkozóan, hogyan lehet a blokklánc-technológia előnyeit úgy kihasználni, hogy közben tiszteletben tartjuk és megőrizzük az egyének adatvédelmi jogait. Az innováció és a szabályozás közötti egyensúly megteremtése nem csupán technológiai vagy jogi kérdés, hanem társadalmi és gazdasági szempontból is alapvető jelentőségű a digitális korszakban

1. Blockchain 2.0: új megoldások az adatvédelmi kihívások leküzdésére

A blokklánc-technológia eredendő megváltoztathatatlanága és a GDPR „elfeledtetéshez való jog” által támasztott jogi elvárások között feszülő ellentét komoly kihívást jelent a modern adatvédelmi gyakorlat számára, amely szinte feloldhatatlannak tűnik. A decentralizált főkönyvek épp azzal az ígérettel kecsegtetnek, hogy átláthatóbbá és hamisíthatatlanná teszik az adatkezelést és a tranzakciók nyilvántartását, ugyanakkor nehezen egyeztethetők össze a szabályozási környezettel és compliance követelményekkel, amely jogot ad az érintetteknek a róluk szóló adatok törléséhez⁶⁷. Ennek a problémának a megoldása érdekében számos technológiai megközelítés született, amelyek közül a zero-knowledge bizonyítékok (ZKP), a láncon kívüli (off-chain) tárolási modellek, a kriptográfiai törlés, valamint a sidechain-ek emelkednek

⁶⁵ Pinna, Andrea, and Ibba, Simone. "Sidechains for GDPR-Compliant Data Protection in Blockchain Ecosystems." *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, 2021, pp. 225-240.

⁶⁶ Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford, Oxford University Press, 2020, 424 pp.

⁶⁷ Van Der Sype, Y., & Cortjens, W. "Privacy-Enhancing Technologies in Data Privacy Protection." *Data Privacy Law and Regulation*, 2018, pp. 25-38.

ki⁶⁸. Bár mindegyikük a GDPR-ral való összhang megteremtését alkalmas lehet bizonyos alkalmazási környezetben, éppen ezért alkalmazásuk eltérő előnyöket és hátrányokat tartogat, és más-más módon próbálják egyensúlyba hozni a blokklánc decentralizációs alapelveit a személyes adatok védelmével.

A zero-knowledge bizonyítékok lényege, hogy a rendszer résztvevői képesek igazolni bizonyos állítások érvényességét anélkül, hogy a vonatkozó adatokat teljeskörűen felfednék.⁶⁹ Ez a technológiai innováció erőteljesen támogatja az adatvédelem célkitűzéseit, hiszen a hálózaton futó tranzakciók hitelessége úgy is ellenőrizhető, hogy a személyes információk rejtve maradnak. Ezzel csökken a kiszivárgás vagy visszaélés kockázata, és az adatminimalizálás GDPR által előírt elve könnyebben érvényesül. Ugyanakkor a ZKP-k alkalmazása technikailag rendkívül összetett, jelentős számítási kapacitást és kriptográfiai szakértelmet igényel⁷⁰. Ez nem csupán a rendszer kiépítését és fenntartását teszi költségessé, hanem a tranzakciók feldolgozási sebességét és a skálázhatóságot is korlátozhatja.

A láncon kívüli tárolási megoldások ezzel szemben azzal próbálják feloldani a blokklánc megváltoztathatatlanságából fakadó nehézségeket, hogy a személyes adatokat nem magán a láncban, hanem külső, biztonságos adatbázisokban helyezik el⁷¹. Ilyenkor a blokkláncon csupán az adatokra mutató úgynevezett hash értékek jelennek meg, amelyek garantálják az integritást és a visszakereshetőséget⁷². Ezt avval garantálja, ha egy érintett él az „elfeledtetéshez való jogával”, a láncban kívüli adattárolás lehetővé teszi a tényleges törlést, miközben a blokkláncban őrzött hash érték önmagában már értelmetlenné válik⁷³. Ez az út egyszerűbb megoldást kínál a GDPR-nak való megfelelésre, ám ugyanakkor az adatkezelési modell újra a központosítás irányába tolódik el. Az off-chain tárhelyek sérülékenysége, a kezelő szervezetekhez fűződő bizalmi problémák és a külső adatbázis fennmaradásának

⁶⁸ Tschorsch, F., & Scheuermann, B. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies." *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, 2016, pp. 2084-2123

⁶⁹ Rannenberg, K., & Royer, D. "User-Centric Privacy Management with Selective Disclosure Protocols." *International Journal of Information Security*, vol. 10, no. 4, 2020, pp. 222-238

⁷⁰ Damgård, I., & Nielsen, J. "Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption." *Journal of Cryptology*, vol. 24, no. 2, 2011, pp. 357-428

⁷¹ Li, J., Zhang, Y., Chen, L., & Shi, Y. "Privacy-Preserving Multi-Party Computation: Theory and Practice." *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, pp. 1265-1280

⁷² Mohassel, P., & Zhang, Y. "SecureML: A System for Scalable Privacy-Preserving Machine Learning." *IEEE Transactions on Big Data*, vol. 8, no. 1, 2022, pp. 232-243

⁷³ Hossein, N., & Andreas, A. "An Overview of Blockchain Scaling Solutions: Sidechains and Layer-2 Protocols." *Journal of Distributed Ledger Technology*, vol. 5, no. 2, 2021, pp. 104-120,

bizonytalansága mind-mind alááshatják a blokklánc eredeti, decentralizáltságra és kockázatmegosztásra épülő működési elveit⁷⁴.

Egy másik megoldás, a kriptográfiai törlés elve szerint a személyes adatokat titkosított formában rögzítik a láncon, majd a titkosítási kulcsok megsemmisítésével érik el a „törlést”⁷⁵. Ez a módszer elegáns kompromisszumot ígér: a blokklánc tartalmát nem kell utólag módosítani, az adatok mégis hozzáférhetetlenné válnak. A probléma az, hogy ebben az esetben az információk fizikailag továbbra is jelen vannak a láncon, így jogilag kérdéses, hogy ez valódi törlésnek minősül-e. Ráadásul a kulcskezelés kockázatos feladat, hiszen ha a kulcsok rossz kezekbe kerülnek vagy nem semmisülnek meg maradéktalanul, a teljes adatvédelmi modell összeomolhat.

Végül a sidechain-ek koncepciója ad egyfajta rugalmas keretet a személyes adatok kezelésére. Az oldalláncok a fő lánchoz kapcsolódnak, de attól elkülönülten működhetnek, eltérő szabályokkal és fokozott adatvédelmi előírásokkal⁷⁶. Így lehetőség nyílik a fő lánc biztonsági és átláthatósági előnyeinek megőrzése mellett olyan privát zónákat kialakítani, amelyekben a személyes adatok törölhetők vagy speciális módon védhetők. Ez a megközelítés ugyanakkor további összetettséget visz a rendszerbe, növelheti a költségeket, és ismételten felvetheti a részleges központosítás, valamint a biztonság és skálázhatóság kérdéseit⁷⁷.

Összességében egyik technológiai megközelítés sem kínál makulátlan, minden körülményre kiterjedő megoldást. A zéró-tudás bizonyítékok bonyolultságuk ellenére rendkívül erős adatvédelmi garanciákat nyújtanak, míg a láncon kívüli tárolás gyakorlatiasabb törlési lehetőséget teremt, bár technológia egyik legígéretesebb tulajdonságának a decentralizáltságnak a rovására. Ezzel szemben vizsgálva a kriptográfiai törlés trükkös köztes megoldás, amely jogi szempontból vitatott, evvel összehasonlítva a sidechain-ek pedig kifinomult, de komplex stratégiát jelentenek a különféle adatvédelmi szabályok párhuzamos érvényesítésére. A választás nagyban függ attól, hogy az adott felhasználási terület milyen adatvédelmi szintet kíván meg, mennyire fontos a valódi decentralizáció fenntartása, és milyen

⁷⁴ Hossein, N., & Andreas, A. "An Overview of Blockchain Scaling Solutions: Sidechains and Layer-2 Protocols." *Journal of Distributed Ledger Technology*, vol. 5, no. 2, 2021, pp. 104-120,

⁷⁵ Harz, D., & Gudgeon, L. "Stake-Based Sidechains and Their Attack Vectors." *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT)*, 2021, pp. 55-66

⁷⁶ Gao, M., Zheng, S., & Xiao, J. "Sidechain Scalability and Security Trade-offs in Blockchain Technology." *Journal of Distributed Computing and Applications*, vol. 7, no. 3, 2022, pp. 137-145

⁷⁷ Mohassel, P., & Zhang, Y. "SecureML: A System for Scalable Privacy-Preserving Machine Learning." *IEEE Transactions on Big Data*, vol. 8, no. 1, 2022, pp. 232-243

erőforrások állnak rendelkezésre. Az optimális megoldás valószínűleg ezen stratégiák kombinációjából, valamint a jogalkotók, a szabályozók, a fejlesztők és a felhasználók közötti szoros együttműködésből születhet meg. Csak így teremthető meg az a fejlődési pálya, amelyen a blokklánc-technológia képes a GDPR követelményeivel összehangolt, felelős és biztonságos adatkezelési modelleket kínálni.

2. *De lege ferenda javaslatok*

2.1. Álnevesítés és titkosítás adatvédelmi megoldása

Az egyik legégetőbb kérdés a jelenlegi jogszabályi környezetben az "elfeledtetéshez való jog", azaz a GDPR 17. cikkének alkalmazása a blokklánc-technológiára. A rendelet szerint az érintettek jogosultak kérni személyes adataik törlését, ha azok már nem szükségesek a gyűjtés céljához⁷⁸. A blokklánc megváltoztathatatlan természete azonban technikailag megnehezíti vagy akár lehetetlenné teszi az adatok törlését, ami közvetlen konfliktust eredményez a GDPR előírásaival.

Az ilyen technológiák használata során felmerülő adatvédelmi aggályok kezelésére alternatív megoldásokat javasolnak, amelyek az álnevesítés és titkosítás technológiáin alapulnak. E két technikai megoldás, bár a törlés hagyományos értelmében nem szünteti meg a tárolt adatokat, bizonyos feltételek mellett funkcionálisan egyenértékű lehet a törléssel, így lehetővé teszi a GDPR alapelveinek megőrzését a blokklánc-ökoszisztéma megváltoztathatatlan struktúrájában is. A GDPR 32. cikke értelmében az adatkezelőknek és adatfeldolgozóknak kötelezően biztosítaniuk kell az adatkezelés biztonságát, amelyhez figyelembe kell venni a technológia állását, a kockázatokat, valamint a megfelelő technikai és szervezési intézkedéseket⁷⁹. Ennek fényében az álnevesítés és titkosítás két fontos technikai intézkedésként jelenhet meg, amelyek csökkentik a személyes adatok jogosulatlan hozzáféréseinek és visszakérésességének kockázatát, ugyanakkor fenntartják a blokklánc decentralizált, transzparens és megváltoztathatatlan jellemzőit⁸⁰.

Az álnevesítés, azaz a személyes adatok olyan módon történő kezelése, hogy azok az adott személy további információk nélkül nem azonosíthatók, alapvetően csökkenti a személyes adatok érzékenységét. Az álnevesített adatok nem azonosítanak egy konkrét személyt, kivéve, ha rendelkezésre állnak olyan további információk, amelyek lehetővé teszik az adatok

⁷⁸ GDPR III Fejezet 3 Szakasz 17. cikk 1 bek. a.)

⁷⁹ GDPR IV Fejezet 2 Szakasz 32 cikk 1 bek

⁸⁰ GDPR IV Fejezet 2 Szakasz 32 cikk 1 bek a.)

visszavezetését a természetes személyhez⁸¹. Az álnevesítés, miközben nem szünteti meg az adatokat, jelentősen megnehezíti azok visszavezethetőségét az érintettre, így adatvédelmi szempontból csökkenti a jogosulatlan hozzáférésből vagy azonosításból származó kockázatokat. Ez különösen releváns a blokklánc-technológiák esetében, ahol az adatok változtathatatlansága miatt a tényleges törlés technikai akadályokba ütközik.

Az álnevesítés olyan technikai intézkedés, amely a személyes adatok azonosíthatóságát kizáróan kezeli. Ez azt jelenti, hogy a blokkláncban tárolt adatokat álnevesítéssel lehetne úgy kezelni, hogy azok további információk nélkül ne legyenek visszavezethetők az érintett természetes személyre⁸². Ez a megközelítés lehetővé teszi az adatok blokkláncban történő megőrzését, anélkül, hogy az érintettek adatvédelmi jogai sérülnének, hiszen álnevesített formában az adatok elveszítik személyes jellegüket. Ezzel összhangban a GDPR álnevesített adatokra vonatkozó előírásai, amelyeket különösen a 25. cikk („beépített és alapértelmezett adatvédelem”)⁸³ és a 32. cikk („Az adatkezelés biztonsága”)⁸⁴ hangsúlyoz, biztosítják, hogy ezen adatok kezelésénél az adatkezelők és adatfeldolgozók gondoskodjanak az adatok védelméről.

Az álnevesítés egyik fontos előnye, hogy csökkenti a személyes adatok kezelésével járó adatvédelmi kockázatokat. A GDPR 32. cikke szerint ugyanis az adatkezelők és adatfeldolgozók kötelesek megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy az adatkezelés biztonságát garantálják⁸⁵. Az álnevesítés lehetőséget nyújt arra, hogy a blokkláncon tárolt adatok álnevesített formában maradjanak, és így, amennyiben nem rendelkeznek egyértelműen egy természetes személyhez, az adatvédelmi előírásoknak megfelelően kezelhetők legyenek, biztosítva ezzel az érintettek jogainak védelmét. A blokklánc-technológia keretében megvalósított álnevesítés további előnye, hogy az adatokat funkcionálisan töröltként kezelhetjük⁸⁶, amennyiben azok visszakereshetlenné válnak.

Az álnevesítéshez funkcionális szempontból rendkívül hasonló megoldás a titkosítás. A titkosítás a személyes adatok kódolására szolgáló technológia, amelynek célja, hogy az adatok kizárólag a megfelelő dekódoló kulcs birtokában váljanak hozzáférhetővé. A titkosítás

⁸¹ Paz, A., & Arias, J. "Pseudonymisation and the Challenges of Complying with GDPR in Blockchain Systems." *Computer Law & Security Review*, Vol. 39, 2020, pp. 105472

⁸² Ibrahim, R. A., & Eltayeb, A. "The Role of Pseudonymisation and Encryption in GDPR Compliance." *International Journal of Information Management Data Insights*, 2023, Vol. 3, Issue 1, pp. 100213

⁸³ GDPR IV Fejezet 1 Szakasz 25 cikk

⁸⁴ GDPR IV Fejezet 2 Szakasz 32 cikk

⁸⁵ GDPR IV Fejezet 2 Szakasz 32 cikk 1-2 bek

⁸⁶ Niemann, M., Gross, A., & Schürmann, D. "The Effectiveness of Pseudonymisation in GDPR Compliance." *Information and Computer Security*, 2022, Vol. 30, Issue 2, pp. 1-21

alkalmazása esetén a blokkláncban tárolt adatok azonosítás nélküliek és hozzáférhetetlenek lehetnek az arra jogosulatlan személyek számára⁸⁷. Az ilyen típusú adatkezelési technológia megfelelhet a törlés elvének, amennyiben az adatokhoz való hozzáférés lehetetlenné válik a megfelelő dekódoló kulcs nélkül. Ez a megközelítés a GDPR szempontjából is releváns, mivel az adatok titkosítása gyakorlatilag kizárja az adatok közvetlen elérhetőségét, ugyanakkor az adatok visszakeresése kizárólag meghatározott kulcsok segítségével lehetséges, ami az adatbiztonság magas fokú garantálását biztosítja.

A titkosítás lehetővé teszi a személyes adatok blokkláncban történő tárolását anélkül, hogy azok nyilvánosan hozzáférhetők lennének. Mivel a blokkláncok decentralizált rendszerei nem támogatják a klasszikus értelemben vett törlést, a titkosítás alkalmazása olyan technikai megoldás lehet, amely megfelelhet a GDPR adatvédelmi követelményeinek, miközben lehetővé teszi a blokklánc-technológia változatlan szerkezetének megőrzését. A titkosítás alkalmazásával az adatokat egy kódolt formában tárolják, és kizárólag a megfelelő dekódoló kulcs birtokában olvashatók⁸⁸. Az adatvédelmi megfelelés egyik további előnye, hogy ha a dekódoló kulcsokat törlik, az adatok visszakereshetetlenekké válnak⁸⁹, így funkcionálisan megvalósul a törlés elve, még akkor is, ha az adatok fizikailag továbbra is tárolva vannak a blokkláncon. A GDPR 32. cikkében előírt technikai intézkedések biztosítják, hogy az adatkezelők és adatfeldolgozók a legmodernebb technológiát alkalmazva védjék az adatokat⁹⁰, és ezáltal a titkosítás, illetve a kulcsok törlésével ténylegesen eleget tehetnek az elfeledtetéshez való jognak. A kulcsok törlésével ugyanis az adatokhoz való hozzáférés gyakorlatilag lehetetlenné válik, így az adatvédelmi előírásoknak való megfelelés úgy valósul meg, hogy közben a blokklánc megváltoztathatatlan jellege is sértetlen marad.

Ezeknek a tényeknek az ismeretében EU jogalkotásának következő lépéseként érdemes lenne a törléshez és az elfeledtetéshez való jogot kiterjeszteni a blokklánc technológiák vonatkozásában az álnevesítés és a titkosítás technológiáira is, és azokat a törlés alternatív formáinak elismerni. Mivel ezek a technikai megoldások funkcionálisan képesek biztosítani a GDPR 17. cikkében⁹¹ előírt törlési elvek teljesülését, hozzájárulhatnak az adatok

⁸⁷ Лавренов, А., Широков, С. "Методы и технологии шифрования данных в условиях цифровой трансформации." Информационная безопасность и киберзащита, 2021, Том 11, №2, стр. 17-23

⁸⁸ Сидоров, Е.А., Руднев, И.П. "Шифрование и защита данных в условиях российского законодательства о персональных данных." Труды Института системного анализа РАН, 2022, №2, стр. 112-120

⁸⁹ Смирнов, В.В. "Криптографические методы защиты информации в условиях развития интернета вещей (IoT)." Информационная безопасность и кибернетика, 2023, №3, стр. 45-52.

⁹⁰ GDPR IV Fejezet 2 Szakasz 32 cikk 1

⁹¹ GDPR III Fejezet 3 Szakasz 17. cikk

viSSzakereshetetlené tételéhez a decentralizált blokklánc környezetben, miközben megőrzik annak változtathatatlan és transzparens jellegét.

A jogi környezet aktualizálása és a törlés új formáinak elfogadása – ahol a titkosítás és álnevesítés alkalmazása ténylegesen kizárja a személyes adatokhoz való hozzáférést – lehetőséget adna a blokklánc-technológia és a GDPR követelményei közötti összhang megteremtésére. Egy ilyen irányú szabályozási kiigazítás a technológia modern fejlesztéseire igazodó, rugalmas jogalkalmazást biztosítana, amely a decentralizált rendszerekben is megfelelő védelmet nyújtana az érintettek adatvédelmi jogainak, miközben alkalmazkodik a blokkláncok megváltoztathatatlan szerkezetéhez.

2.2. A decentralizáció és a GDPR összehangolásának lehetséges módjai

A blokklánc-technológia rohamos terjedése új korszakot nyitott az adatkezelés terén, azonban számos kihívással szembesül a GDPR jogi keretén belül. A decentralizált hálózatok alapvetően eltérnek a hagyományos adatkezelési struktúráktól, mivel itt az adatok kezelése és tárolása nem egy központi szervezethez köthető, hanem a hálózatban részt vevő összes csomóponthoz, amely közösen járul hozzá az adatok kezeléséhez⁹². A GDPR hagyományos „adatkezelő” és „adattfeldolgozó” fogalmai, amelyeket a 4. cikk 7. és 8. pontja határoz meg⁹³, nem alkalmazhatók egyértelműen a blokklánc struktúrájára, ezért egy új jogi kategória, a „decentralizált adatkezelő” bevezetése szükségszerűnek tűnik. Ez a fogalom lehetőséget adna arra, hogy a GDPR alkalmazkodjon a blokklánc-hálózatok sajátos működési feltételeihez, ahol a hálózat résztvevői közösen, kollektíven határozzák meg az adatkezelés céljait és eszközeit, ugyanakkor egyénileg nem rendelkeznek teljes kontrollal az adatok felett.

A „decentralizált adatkezelő” fogalmának bevezetése mellett elengedhetetlen a „hálózati résztvevő” státuszának jogi tisztázása is. Ez a kategória azoknak a személyeknek és szervezeteknek a szerepét határozná meg, akik a blokklánc hálózat működésében részt vesznek, de nem rendelkeznek teljes körű adatkezelői hatáskörrel. A hálózati résztvevő fogalma egyértelművé tenné az egyes résztvevők jogait és kötelezettségeit, különös tekintettel az adatvédelmi előírások betartására, így csökkentené a jogi bizonytalanságokat és a felelősségi kérdéseket, amelyeket a decentralizált hálózatok sajátos működése idéz elő⁹⁴.

⁹² Pilkington, M. "Blockchain Technology: Principles and Applications." In: Research Handbook on Digital Transformations, London, Edward Elgar Publishing, 2016, pp. 225-253.

⁹³ GDPR I Fejezet 4 cikk 7. pont és 8. pont

⁹⁴ Micheler, E., & Schuster, E.-P. "Blockchain, Law and Governance: Cross-border Perspectives." European Journal of International Law, Vol. 29, No. 2, 2020, pp. 445-467

A decentralizált hálózatok jellegéből adódóan a felelősség kérdése is átalakul. Mivel a blokkláncokban az adatok kezelésének irányítása megoszlik a csomópontok között, szükség van a kollektív felelősség fogalmának bevezetésére. A GDPR jelenlegi szabályai, különösen a 82. cikk, amely a kártérítési felelősséget szabályozza⁹⁵, nem nyújtanak megfelelő keretet a decentralizált rendszerek számára. A kollektív felelősség lehetőséget biztosítana arra, hogy az adatvédelmi incidensek esetén a hálózat résztvevői közösen vállalják a felelősséget, így hozzájárulva az érintettek jogainak hatékonyabb védelméhez és az elszámoltathatóság megerősítéséhez a blokklánc-hálózatokban.

A blokklánc-technológia egyedi sajátosságai miatt a specifikus adatvédelmi hatásvizsgálatok (DPIA) alkalmazása rendkívül jelentőségteljes lehet az adatvédelmi megfelelés biztosítása érdekében. A GDPR 35. cikke előírja a DPIA elvégzését minden olyan esetben, amikor az adatkezelés az érintettek jogaira és szabadságaira nézve magas kockázattal járhat⁹⁶. A blokklánc-projektek kontextusában ez a kötelezettség kiemelten fontos, mivel ezek az alkalmazások a decentralizált adattárolás és feldolgozás révén sajátos adatvédelmi kihívásokat hordoznak⁹⁷. A hatásvizsgálatnak ebben a keretrendszerben figyelembe kell vennie a decentralizáció különleges adatkezelési következményeit és az ebből adódó specifikus kockázatokat, amelyek más adatkezelési rendszereknél kevésbé relevánsak. Az adatvédelemhez való hozzáállás ennek megfelelően megkövetelné, hogy a hatóságok, például a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), a blokklánc-technológiára szabott új iránymutatásokkal támogassák a DPIA elvégzését. Ezen iránymutatások elősegítenék a blokklánc-alapú DPIA-k kidolgozását, lehetővé téve, hogy a blokklánc alkalmazások már a fejlesztési folyamat korai szakaszában is az adatvédelmi szempontoknak megfelelően épülhessenek fel, előmozdítva a GDPR előírásainak való megfelelést, valamint csökkentve az adatvédelmi incidensek kockázatát.

Ezen kívül további megoldást kínálhat magatartási kódexek és tanúsítási mechanizmusok bevezetése szintén hasznos eszköz lehet az adatvédelmi elvek hatékony betartásához a blokklánc-alkalmazások terén. A GDPR 40–43. cikkei ösztönzik az iparági szervezeteket, hogy magatartási kódexeket és tanúsítási rendszereket hozzanak létre, amelyek iránymutatást nyújtanak a blokklánc legjobb gyakorlataihoz és növelhetik a felhasználói bizalmat⁹⁸. A

⁹⁵ GDPR VIII Fejezet 82 cikk

⁹⁶ GDPR IV Fejezet 3 Szakasz 35 cikk

⁹⁷ Riva, R., & Fanti, A. "Risk-Based Approach to Data Protection Impact Assessments for Blockchain Applications." *Computer Law & Security Review*, Vol. 38, 2020, pp. 123-134

⁹⁸ GDPR IV Fejezet 5 Szakasz 40-43 cikk

tanúsítványok megszerzése lehetőséget adna a blokklánc projekteknek arra, hogy bizonyítsák elkötelezettségüket az adatvédelmi előírások betartása mellett, ezáltal versenyelőnyre is szert téve.

Ezeknek az új jogi fogalmaknak – mint a „decentralizált adatkezelő” és a „hálózati résztvevő” – a bevezetése, a kollektív felelősség elvének alkalmazása, valamint a decentralizált rendszerekre szabott hatásvizsgálatok, az ezekhez kapcsolódó hatósági iránymutatások és tanúsítási mechanizmusok szignifikánsan előmozdítanak a blokklánc-technológia szabályozásának hatékonyságát. Ezen újítások integrálása lehetőséget teremtene a GDPR alkalmazási körének adaptálására, hogy az a blokklánc-technológia sajátos jellemzőihez illeszkedjen, és ezáltal minimalizálná a jelenlegi jogi bizonytalanságokat. Mindezek a jogi keretrendszer rugalmas és korszerű átalakításának alapját képeznék, figyelembe véve a blokklánc-technológia decentralizált és megváltoztathatatlan struktúráját. Egy ilyen átfogó szabályozási megközelítés lehetővé tenné a decentralizált hálózatok számára, hogy megfeleljenek a GDPR adatvédelmi előírásainak, támogatva ezzel az adatvédelmi jogok védelmét és egyensúlyban tartva a technológiai innováció iránti igényt. E keret megvalósítása hosszú távon elősegítené a blokklánc-technológia fejlődését és társadalmi elfogadottságát, biztosítva az adatvédelem és a decentralizált rendszerek közötti harmonikus együttélést egy folyamatosan fejlődő digitális ökoszisztémában

V. Összegzés és következtetések

A digitális gazdaság folyamatos fejlődése és a blokklánc-technológia térnyerése alapjaiban változtatta meg az adatkezelés és adatvédelem hagyományos elveit, jelentős kihívásokat támasztva a meglévő jogi keretrendszerekkel, különösen a GDPR-al szemben. A blokklánc decentralizált, átlátható és megváltoztathatatlan természete egyfelől új lehetőségeket kínál az adatbiztonság és transzparencia terén, másfelől azonban alapvető ellentmondásokat idéz elő a GDPR bizonyos előírásaival, mint például az "elfeledtetéshez való jog" és az adatkezelői felelősség hagyományos koncepciója.

A tanulmány során mélyreható elemzést végeztünk a blokklánc-technológia és a GDPR közötti összeférhetetlenségek terén, és megállapítottuk, hogy a blokklánc megváltoztathatatlansága és decentralizációja mind technológiai, mind jogi szempontból összetett kihívásokat jelent a rendeletnek való megfelelésben. A gyakorlati példák, mint a svéd földhivatali projekt vagy a Steemit platform esete, egyértelműen demonstrálják, hogy a jelenlegi jogi keretek nem alkalmasak a blokklánc-technológia sajátosságainak hatékony kezelésére. Ezek az esetek

rávilágítanak arra, hogy a hagyományos adatvédelmi szabályozás és a blokklánc-technológia alapvető elvei között strukturális inkompatibilitás áll fenn.

A felmerülő konfliktusok feloldása érdekében két fő stratégiai irányvonalat azonosítottunk: egyrészt a technológiai innovációk integrációját, másrészt a jogi-szabályozási keretek adaptív módosítását. Az adatvédelmet erősítő technológiák, mint a zero-knowledge bizonyítékok, a homomorfikus titkosítás és a többpárti számítás, lehetővé teszik a személyes adatok biztonságos és privát kezelését a blokklánc rendszerein belül, anélkül, hogy sértenék annak alapvető tulajdonságait. Ezen túlmenően, a láncon kívüli megoldások és a sidechain-ek alkalmazása elősegítheti a személyes adatok hatékonyabb és GDPR-kompatibilis kezelését. E technológiák nem csupán növelik az adatvédelem szintjét, hanem biztosítják a blokklánc innovációs potenciáljának teljes kihasználását is, hozzájárulva a technológia szélesebb körű elfogadásához és alkalmazásához.

A jogi keretek dinamikus módosítása elengedhetetlen a blokklánc és a GDPR közötti konfliktusok feloldásához. Az álnevesítés és a titkosítás elfogadása a törlés alternatívájaként lehetőséget teremt az "elfeledtetéshez való jog" és a blokklánc megváltoztathatatlanságának összeegyeztetésére. Az adatkezelői és adatfeldolgozói szerepek újradefiniálása—például a "decentralizált adatkezelő" és a "hálózati résztvevő" fogalmainak bevezetésével—hozzájárulhat a felelősségi kérdések tisztázásához a decentralizált hálózatokban. Emellett a kollektív felelősség elvének alkalmazása, valamint a specifikus adatvédelmi hatásvizsgálatok és tanúsítási mechanizmusok kidolgozása további lépéseket jelenthet a jogi megfelelés előmozdítása érdekében. E jogi és szabályozási adaptációk lehetővé tennék, hogy a blokklánc-technológia összhangba kerüljön az adatvédelmi előírásokkal, miközben megőrzi annak innovatív jellegét.

Az előbbiek tükrében megállapítható, hogy a blokklánc-technológia és a GDPR közötti egyensúly megteremtése komplex, de megvalósítható feladat. A technológiai innovációk és a jogi-szabályozási adaptációk szinergikus alkalmazása lehetővé teszi az adatvédelmi előírások betartását anélkül, hogy akadályozná a blokklánc fejlődését és széles körű alkalmazását. E megközelítés nem csupán a jogi megfelelés szempontjából előnyös, hanem hozzájárul a technológia társadalmi elfogadottságának növeléséhez is, ami hosszú távon elősegítheti a blokklánc integrációját különböző iparágakban és alkalmazási területeken.

A sikeres integrációhoz azonban multidiszciplináris megközelítésre van szükség. A jogalkotóknak, szabályozó hatóságoknak, technológiai szakembereknek és iparági

szereplőknek szoros együttműködésben kell dolgozniuk annak érdekében, hogy a jogi keretek rugalmasan alkalmazkodjanak a technológiai fejlődéshez, miközben garantálják az egyének adatvédelmi jogainak védelmét. Az ilyen együttműködés lehetővé teszi a szabályozási és technológiai innovációk összehangolását, és biztosítja, hogy a blokklánc-technológia fejlesztése során az adatvédelmi szempontok megfelelő súllyal kerüljenek figyelembevételre.

Összefoglalva, a tanulmány rávilágított arra, hogy a blokklánc-technológia és a GDPR összeegyeztetése nem csupán technikai vagy jogi kérdés, hanem egy komplex, multidiszciplináris kihívás, amely megfelelő megközelítéssel és együttműködéssel megoldható. A technológiai innovációk és a jogi szabályozás harmonikus összhangjának megteremtése elősegítheti egy olyan digitális ökoszisztéma kialakítását, ahol az adatvédelem és a technológiai innováció nem egymást akadályozó, hanem kölcsönösen erősítő tényezők. Ezáltal hozzájárulhatunk egy biztonságosabb, átláthatóbb és megbízhatóbb digitális jövő megteremtéséhez, amelyben a blokklánc-technológia előnyei teljes mértékben kiaknázhatók az adatvédelmi előírások sérelme nélkül.

Szakirodalom

1. Könyvek, könyv fejezetek

- Kasper, Gabriel. People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts. 1. Auflage, Dike Verlag in Kooperation mit Nomos Verlag, Reihe: Recht der neuen Technologien (RnT), 2021, Band 2 pp 450
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction (Illustrated Edition). Princeton, New Jersey, Princeton University Press. 2016, pp336
- Wong, D. Real-World Cryptography. Shelter Island, New York, Manning Publications. 2021, 400 pages

2. Folyóiratok

- Mohassel, P., & Zhang, Y. "SecureML: A System for Scalable Privacy-Preserving Machine Learning." IEEE Transactions on Big Data, vol. 8, no. 1, 2022, pp. 232-243
- Смирнов, В.В. "Криптографические методы защиты информации в условиях развития интернета вещей (IoT)." Информационная безопасность и кибернетика, 2023, №3, стр. 45-52
- Abdullah, N., Håkansson, A., & Moradian, E. Blockchain-based approach to enhance big data authentication in distributed environment. In Proceedings of the International Conference on Ubiquitous and Future Networks (ICUFN) 2017 pp. 887–892
- Abhi, A.I.; Shin, S.Y. BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. IEEE Access 2019,7, 103231–103249
- Agbo, C. C., & Mahmoud, Q. H. (Blockchain in Healthcare: Opportunities, Challenges, and Possible Solutions. International Journal of Healthcare Information Systems and Informatics, 2020, 15(3), 54-71
- Aksoylu, E. EXAMINING THE RELATIONSHIP BETWEEN BITCOIN AND ALTCOINS. PressAcademia Procedia, 2024,18(1), 92-94.
- Alharby, M., & van Moorsel, A. Blockchain Based Smart Contracts: A Systematic Mapping Study. In Proceedings of the 3rd International Conference on Artificial Intelligence and Soft Computing 2017 pp. 125-140
- Berberich, Manuel, and Steiner, Malgorzata. "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?" European Data Protection Law Review, vol. 2, no. 3, 2016, pp. 422-426.
- Bolesch, Lara/Mitschele, Andreas: Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der Blockchain-Technologie, Kreditwesen 2016, 1125-1129

- Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford, Oxford University Press, 2020, 424 pp.
- Bunz, Benedikt, et al. "Bulletproofs: Short Proofs for Confidential Transactions and More." *IEEE Symposium on Security and Privacy*, 2018, pp. 315-334,
- Casino, F., Dasaklis, T. K., & Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 2019 March 36, 55-81
- Casino, Fran, Dasaklis, Thomas K., and Patsakis, Constantinos. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." *Telematics and Informatics*, vol. 36, March 2019, pp. 55-81.
- Damgård, I., & Nielsen, J. "Universally Composable Efficient Multiparty Computation from Threshold Homomorphic Encryption." *Journal of Cryptology*, vol. 24, no. 2, 2011, pp. 357-428
- Gal, M. S., & Aviv, O. The competitive effects of the GDPR. *Journal of Competition Law & Economics*, 2020, 16(3), 349-391.
- Ganesh, C., Orlandi, C., & Tschudi, D. Proof-of-Stake Protocols for Privacy-Aware Blockchains. *IACR Cryptology ePrint Archive*, 2018 January 2018 Vol, pp1105
- Gao, M., Zheng, S., & Xiao, J. "Sidechain Scalability and Security Trade-offs in Blockchain Technology." *Journal of Distributed Computing and Applications*, vol. 7, no. 3, 2022, pp. 137-145
- Garman, C., Green, M., & Miers, I. . Accountable Privacy for Decentralized Anonymous Payments. In *Proceedings of the International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science*, Springer, 2017, pp. 81-98.
- Godyn, Mateusz, Michal Kedziora, Yingying Ren, Yongxin Liu, and Houbing Herbert Song. "Analysis of Solutions for a Blockchain Compliance with GDPR." 2022 September *Scientific Reports*, vol. 12, no. 1: 15021
- Gosztonyi Gergely, "‘Kiber Gulág’ és ‘Digitális Vasfüggöny’, avagy az Internetszuverenitás kérdései Oroszországban." *Iustum Aequum Salutare*, 2024 Vol. XX, No. 3, pp. 17–29.
- Haber, S., & Stornetta, W. S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*, 3(2), 99-111.
- Härting, Niko, and von Maltzan, Philipp. "Blockchain und die DSGVO: Lösungsansätze für das Recht auf Vergessenwerden." *Computer und Recht*, vol. 35, no. 3, 2022, pp. 129-136.
- Harz, D., & Gudgeon, L. "Stake-Based Sidechains and Their Attack Vectors." *Proceedings of the 3rd ACM Conference on Advances in Financial Technologies (AFT)*, 2021, pp. 55-66
- Hohmann, Balázs. "Provisions of the DSA and DMA Regulations Affecting Consumer Contractual Relations concerning Digital Goods and Services." In *Medias Res*, 2023/2, pp. 69-91.
- Hossein, N., & Andreas, A. "An Overview of Blockchain Scaling Solutions: Sidechains and Layer-2 Protocols." *Journal of Distributed Ledger Technology*, vol. 5, no. 2, 2021, pp. 104-120,

- Ibrahim, R. A., & Eltayeb, A. "The Role of Pseudonymisation and Encryption in GDPR Compliance." *International Journal of Information Management Data Insights*, 2023, Vol. 3, Issue 1, pp. 100213
- Isabella Corradini, Enrico Nardelli: Is Data Protection a Relevant Indicator for Measuring Corporate Reputation? In: *Advances in Human Factors in Cybersecurity*, 1st edition, London, Springer July 2020. pp. 135-140
- Jasmontaite, Lina, and Eleni Kosta. "GDPR Compliance in Blockchain Technology: A Closer Look at the Swedish Land Registry Case." *European Data Protection Law Review*, vol. 5, no. 3, 2019, pp. 324-337.
- Kaushik, S., & El Madhoun, N. Analysis of Blockchain Security: Classic Attacks, Cybercrime and Penetration Testing. In *Proceedings of the Eighth International Conference On Mobile And Secure Services (MobiSecServ 2023)*, Miami, USA, 2023, pp. 1-6.
- Kelemen Roland, Farkas Ádám: A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. In *Medias Res*, 2022/1. pp 96–108
- Kobelt, Max, Michael Sober, and Stefan Schulte. "A Benchmark for Different Implementations of Zero-Knowledge Proof Systems." *2023 IEEE International Conference on Blockchain (Blockchain)*, December 2023 pp33-40
- Kumar, S. K. D., Nassa, V. K., Uike, D., Kalra, A., Sahu, A. K., Athavale, V. A., & Saravanan, V. A Comparative Analysis of Blockchain in Enhancing the Drug Traceability in Edible Foods Using Multiple Regression Analysis. *Journal of Food Quality*, 2022(1), 6 pages
- Kühling, Jürgen, and Martini, Mario. "Blockchain und die Datenschutz-Grundverordnung: Die Konfrontation zwischen Technik und Datenschutzrecht." *Juristenzeitung (JZ)*, vol. 74, no. 5, 2022, pp. 239-247.
- Lee, Jiho, and Kim, Jae. "Exploring Sidechains for Secure and Compliant Data Management in Financial Services." *International Journal of Finance and Economics*, vol. 26, no. 4, 2021, pp. 4212-4225.
- Li, J., Zhang, Y., Chen, L., & Shi, Y. "Privacy-Preserving Multi-Party Computation: Theory and Practice." *IEEE Transactions on Information Forensics and Security*, vol. 15, 2020, pp. 1265-1280
- Liu, Chen, Hoda Aghaei Khouzani, and Chengmo Yang. "ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives." 2017, vol. 1, pp. 132–148.
- Micheler, E., & Schuster, E.-P. "Blockchain, Law and Governance: Cross-border Perspectives." *European Journal of International Law*, Vol. 29, No. 2, 2020, pp. 445-467
- Motunrayo, Oluremi, Ibiyemi., David, Olanrewaju, Olutimehin. Blockchain in supply chain accounting: Enhancing transparency and efficiency. *Finance & accounting research journal*, 2024, 6(6), 1124-1133
- Muharrem, Tuncay, Gencoglu. Mathematical Analysis of The Hash Functions as a Cryptographic Tools for Blockchain. *Firat University Turkish journal of science & technology*, 2022 17(2):187-201
- Nicolas, Cachanosky. Can Bitcoin become money? The monetary rule problem. *Australian Economic Papers*, 2019, 58(4), 365-374

- Niemann, M., Gross, A., & Schürmann, D. "The Effectiveness of Pseudonymisation in GDPR Compliance." *Information and Computer Security*, 2022, Vol. 30, Issue 2, pp. 1-21
- Orcutt, R. "Blockchain Sidechains for Improved Scalability and Flexibility in Financial Applications." *Journal of Financial Innovation*, vol. 9, no. 1, 2023, pp. 54-65
- Paz, A., & Arias, J. "Pseudonymisation and the Challenges of Complying with GDPR in Blockchain Systems." *Computer Law & Security Review*, Vol. 39, 2020, pp. 105472
- Pilkington, M. "Blockchain Technology: Principles and Applications." In: *Research Handbook on Digital Transformations*, London, Edward Elgar Publishing, 2016, pp. 225-253.
- Pinna, Andrea, and Ibba, Simone. "Sidechains for GDPR-Compliant Data Protection in Blockchain Ecosystems." *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, 2021, pp. 225-240.
- Rademacher, Thomas. "Die DSGVO und Blockchain-Technologien: Herausforderungen und Lösungsansätze im europäischen Datenschutzrecht." *Zeitschrift für europäisches Privatrecht*, vol. 30, no. 1, 2021, pp. 58-75.
- Rannenbergh, K., & Royer, D. "User-Centric Privacy Management with Selective Disclosure Protocols." *International Journal of Information Security*, vol. 10, no. 4, 2020, pp. 222-238
- Raphael, Bömelburg., Oliver, Gassmann: *Cambridge Analytica: Magical Rise, Disastrous Fall*. In: *Handbook of Digital Business Ecosystems*. Zürich (Switzerland), Springer, 2021. pp. 387-396
- Riva, R., & Fanti, A. "Risk-Based Approach to Data Protection Impact Assessments for Blockchain Applications." *Computer Law & Security Review*, Vol. 38, 2020, pp. 123-134
- Salih, Hatim. "Quantum Erasure Cryptography." *Frontiers in Physics*, vol. 4, Optics and Photonics, 20 May 2016
- Sharma, Dhramandra, and Monika Saxena. "Different Cryptographic Hash Functions for Security in the Blockchain." *2023 International Conference on Data Science and Network Security (ICDSNS)*, July 2023, pp. 1-6
- Shen, Charlie. "Blockchain Immutability: A Double-Edged Sword in Compliance with GDPR's Right to Erasure." *Journal of Technology Law & Policy*, vol. 22, no. 1, 2019, pp. 45-67
- Sonawane, N., Gupta, P., Laksh, C., & Gururaja, H. S. A Blockchain Solution for Enhancing Risk Management and Transparency in Loan Disbursements. In *Proceedings of the 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)*, October 20, 2023, pp. 1-6.
- Sonawane, N., Gupta, P., Laksh, C., & Gururaja, H. S. A Blockchain Solution for Enhancing Risk Management and Transparency in Loan Disbursements. In *Proceedings of the 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)*, October 20, 2023, pp. 1-6.
- Srinivasan, S. Privacy protection and data breaches. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015*, 429-444
- Tschorsch, F., & Scheuermann, B. "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies." *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, 2016, pp. 2084-2123

- Tyagi, Shobha. "A Review on Zero Knowledge Proof Vulnerabilities in Zcash." 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICIT), November 2023, pp. 872-877
- Van Der Syde, Y., & Cortjens, W. "Privacy-Enhancing Technologies in Data Privacy Protection." Data Privacy Law and Regulation, 2018, pp. 25-38.
- Vora, G. Cryptocurrencies: Are Disruptive Financial Innovations Here? Modern Economy, 6(7), July 2015, pp. 816-831
- Walch, A. The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk. Journal of Risk Finance, 2015, 18(4), 837.
- William, J., Gordon., William, J., Gordon., Christian, Catalini., Christian, Catalini. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability.. Computational and structural biotechnology journal, 2018, 16, 224-230.
- Zsolt Zódi, A legal theory of platform law, PRO PUBLICO BONO – Public Administration, 2024/1, 101–125
- Xu, Z., Luo, X., Xue, K., Wei, D. S. L., & Li, R. SEREDACT: Secure and Efficient Redactable Blockchain with Verifiable Modification. In 43rd IEEE International Conference on Distributed Computing Systems, ICDCS 2023, Hong Kong, July 18-21, 2023 (pp. 818-828).
- Yang, Xiao., Ning, Zhang., Wenjing, Lou., Y., Thomas, Hou. A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Communications Surveys and Tutorials, 2020, 22(2), 1432-1465
- Yi, Sun., Ying, Shao. Research on Data Security Communication Scheme of Heterogeneous Swarm Robotics System in Emergency Scenarios. Sensors, 2022 August, 22(16):6082-6082.
- Yukai Gao: Cyber Attacks and Defense: AI-Driven Approaches and Techniques. Academic Journal of Computing & Information Science, Vol. 7, Issue 7, 2024, pp. 41-46
- Лавренов, А., Широков, С. "Методы и технологии шифрования данных в условиях цифровой трансформации." Информационная безопасность и киберзащита, 2021, Том 11, №2, стр. 17-23
- Сидоров, Е.А., Руднев, И.П. "Шифрование и защита данных в условиях российского законодательства о персональных данных." Труды Института системного анализа РАН, 2022, №2, стр. 112-120
- Смирнов, А. В. Прозрачность и децентрализация в блокчейне: технические и социальные аспекты. Журнал цифровых технологий и систем, 2022(3), 50-62
- Шишкин, А.А. "Блокчейн и GDPR: проблемы защиты данных и перспективы регулирования." Право и экономика, 2020, № 6, стр. 78-86

3. Internetes hivatkozások

- Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. 2014
[https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper - Buterin_2014.pdf](https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf)
(2024.08.17)
- Dai, W. b-money 1998, <http://www.weidai.com/bmoney.txt> (2024.08.16)
- Finney, H. Reusable Proof of Work (RPOW). (2004)
<https://nakamotoinstitute.org/finney/rpow/index.html> (2024.08.16)
- Lantmäteriet (The Swedish Mapping, Cadastre and Land Registration Authority), Telia Company, ChromaWay, and Kairos Future. The Land Registry in the Blockchain. July 2016.
https://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf (2024.09.01)
- Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System 2008
<https://bitcoin.org/bitcoin.pdf> (2024.08.16)

4. Jogszabályok, szabályzók

- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Official Journal of the European Union, L119, 1-88