BLOKKLÁNC, OKOSSZERZŐDÉSEK ÉS ADATVÉDELEM

SZERZŐ:DR. ESZTERI DÁNIEL JOGÁSZ, A NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG INCIDENSBEJELENTÉSI OSZTÁLYÁNAK VEZETŐJE, AZ EÖTVÖS LORÁND TUDOMÁNYEGYETEM JOGI TOVÁBBKÉPZŐ INTÉZET ÉS A NEMZETI KÖZSZOLGÁLATI EGYETEM MEGBÍZOTT OKTATÓJA ADATVÉDELMI JOGBÓL, 2015-BEN PH.D. FOKOZATOT SZERZETT A PÉCSI TUDOMÁNYEGYETEMEN A VIRTUÁLIS TULAJDONJOGRÓL ÍRT DISSZERTÁCIÓJÁVAL

1. **A blokklánc alapú adatkezelés**

A blokklánc egy adatok tárolására és kezelésére szolgáló rendszer, az úgynevezett elosztott főkönyvi technológiák egyik képviselője. Olyan tranzakciós adatbázis, amely több számítógépből álló hálózaton oszlik el, nem pedig központi helyen tárolják. A hálózaton nincs alá-fölé rendeltségi viszony az egyes gépek között, amelyek úgynevezett csomópontokként (angolul: node-okként) funkcionálnak és mindegyik csomópont összeköttetésben áll az összes többivel. Az ilyen típusú hálózat előnye, hogy egy csomópont kiesése semmilyen fennakadást nem okoz a rendszer működésében, feladatait azonnal át tudják venni másik csomópontok.

A blokklánc alapú hálózatokon az adatok tárolása az ún. blokkokban történik. Ezek olyan adattárolási egységek, amelyekben bármilyen információ eltárolható, az adott blokklánc létrehozásának céljától függően.

Az információkat tartalmazó blokkok láncszerűen, utólag megváltoztathatatlanul kapcsolódnak egymáshoz, ami annyit jelent, hogy az újabb blokkokat és a bennük lévő új adatokat mindig csak a lánc végére lehet felfűzni.

A rendszer az egyes felhasználók „digitális aláírásaival” látja el a blokkokban tárolt adatokat és azokkal végzett tranzakciókat, műveleteket, és ez alapján ítéli meg, hogy pl. adott blokkban tárolt adathalmaz feletti rendelkezés, vagy hozzáférés joga kit illet meg.

A láncszerűen felépülő és így egyre növekvő adatbázishoz az újabb adatokat újabb blokkokban adják hozzá. A blokkokban tárolt adatokkal végzett valamennyi művelet naplóját is az egyes blokkokban tárolják, a tranzakciók összefoglalása pedig az úgynevezett Merkle-fát eredményezi. Ezen műveletek naplóját nevezzük összefoglaló néven „blokktörténetnek”.

A csomópontok feladata az is, hogy a blokkokban tárolt adatokkal végzett adatkezelési műveletek hitelességét algoritmikus úton ellenőrizzék. A művelet jóváhagyása során azt ellenőrzik, hogy a tranzakció digitálisan megfelelően alá van-e írva a műveletet indítványozó felhasználó által, és van-e bármilyen hiteles előzménye a blokkláncon. Amennyiben a csomópontok (vagy előre meghatározott számú csomópont) jóváhagyják a műveletet, úgy az rögzítésre kerül a blokkban, ami ezentúl megmásíthatatlanul hozzákapcsolódik a teljes lánchoz.

A blokkláncot legegyszerűbben egy olyan adatkezelési technológiának írhatjuk le a fentiek alapján, amely az adatok kezelését egy közös, elosztott hálózaton teszi lehetővé, amely központi ellenőrző szerv felügyelete nélkül is működőképes. Az adatokkal végzett műveletek hitelesítése a hálózaton algoritmikus alapú önellenőrző mechanizmusokkal biztosított.

2.Okosszerződések a blokkláncon

Nick Szabo volt az, aki először - az „okos szerződés” koncepcióját és kifejezését használva 1996-ban az elosztott hálózat adatkezelési műveleteinek automatizálását írta le.

Szabo szerint az okos szerződés olyan szerződés, amely automatikusan megvalósul, ha a korábban meghatározott feltételek teljesülnek, így a szerződés gyakorlatilag „önmagát teljesíti” és ezért megszeghetetlen. A szerződés teljesítését, biztonságát és megszeghetetlenségét egy számítógépes hálózat biztosítja, amelyikben a felek azt elkészítették, ezért nincs szükség a hitelesítéshez harmadik fél (pl. ügyvéd) közreműködésére.

Amint az a gyakorlatban már látható, a blokklánc egy teljesen életképes technológia az okosszerződéses alkalmazások futtatásához: a felhasználók részére automatikus szerződések megkötésének lehetőségét a blokklánc-alapú platform, az Ethereum vezette be először. Lényegében a hálózaton futó program automatikusan végrehajt egy bizonyos döntést, ha a szükséges feltételek teljesülnek.

Az okosszerződések esetében is a csomópontok hitelesítik a folyamatot és az azzal összefüggésben kezelt adatokat, így például egy adásvételnél a szerződő felek számlaszámait, az összeget, az időpontokat (pl. határidő), egyéb feltételeket, de akár más személyes adatokat (pl. név) vagy szöveges egyéb információkat (pl. közlemény) is rögzíteni lehet. A szerződés létrejöttét ugyanúgy a csomópontok hitelesítik algoritmikus módon, az adatok és mozgásuk naplója

pedig megváltoztathatatlanul rögzül a blokkláncban.

Az automatizálásért felelős okosszerződés alkalmazás a hálózat minden résztvevője számára elérhető, hozzáférhető és használható. Az okosszerződések fő célja a legtöbb helyzetben a blokkláncon lévő tranzakciók automatizálása és hitelesítése, ha bizonyos feltételek teljesülnek.

3.A GDPR-nak való megfelelés kérdése

A blokklánc-alapú adatkezelés komoly kihívást okozhat a GDPR (az Európai Unió adatvédelmi rendelete) előírásainak való megfelelést illetően.

Például a célhoz kötöttség elve alapján a személyes adatokat csak meghatározott, egyértelmű és jogszerű célból szabad gyűjteni, és azokat nem szabad az említett célokkal összeegyeztethetetlen módon kezelni. Az adattakarékosság elve szerint pedig a kezelt személyes adatoknak megfelelőnek és relevánsnak kell lenniük az adatkezelés céljai szempontjából és az e célokkal kapcsolatban szükségesre kell korlátozódniuk. Mindkét elv tiltja a túlzott, felhalmozott, szükségtelen adatok kezelését.

A blokklánc működésének egyik alapelve az, hogy az összes adat megőrzési időkorlát nélkül tárolódik az adatbázisban, a velük eszközölt, pl. okosszerződéses műveletek naplójával együtt. Az adatok és azokon végzett adatkezelési műveletek naplója felfűződik a régebbiekre az integritás és a biztonság garantálása érdekében. Az adatokat és tranzakciónaplókat határozatlan ideig tárolják a rendszerben, abból a célból, hogy pontosan nyomon lehessen követni az egyes adatkezelési műveletek és az adatok sorsát. Minden csomópont továbbá az adatbázis teljes másolatát tárolja önellenőrzési célokból. Első látásra ezek a jellemzők ellentétben állnak a GDPR fent említett alapelveivel.

A blokklánc-alapú adatkezelés jogszerűségének megítéléséhez azonban egy fontos előkérdés, hogy az ilyen típusú technológia alkalmazása egyáltalán kompatibilissé tehető-e az bármiféle adatkezelési céllal.Az alapelveknek való megfelelés szempontjából tehát meg kell vizsgálni, hogy a személyes adatok ilyen típusú kezelése (pl. adatok határozatlan ideig történő tárolása a láncban) összeegyeztethető-e bármilyen legitim céllal. Vannak olyan típusú adatkezelések, amelyek alapvetően nem alkalmasak erre. Például egy az érintett hozzájárulásán alapuló adatkezelés (pl. egy direkt marketing célú hírlevél-küldő szolgáltatás)

szinte soha sem lesz ilyen, mivel a GDPR szerinti, a személyes adatok törlésére vonatkozó kötelezettség teljesítése a hozzájárulás visszavonása esetén nem teljesíthető.

A jogszabályi kötelezettség teljesítésén alapuló adatkezelés, például ingatlan-nyilvántartások vagy állami levéltárak vezetése esetén azonban könnyebb a helyzet, hiszen ezeknek az adatbázisoknak a célja az összes személyes adat és az azokkal végzett valamennyi művelet megőrzése és eltárolása, archiválása. A közérdekű archiválási cél tehát könnyebben állhatja ki az alapelvi megfelelés próbáját blokklánc alkalmazása esetén. Egy adott blokklánc-alapú adatkezelés ezért csak eseti alapon értékelhető a jogszerűség és a GDPR-megfelelés szempontjából.

4. Megoldások az adatvédelmi megfelelés érdekében

Mielőtt személyes adatokat kezelésére használnánk a blokkláncot, pontosan tisztáznunk kell, hogy milyen feladatra használjuk fel az adatokat, és ezért korlátozni kell a felhasznált adatok körét a cél szempontjából releváns adatokra. Ez az ún. beépített adatvédelem elvének alkalmazása szempontjából is kulcsfontosságú követelmény.

Habár a személyes adatok törlésének lehetősége jelenti a legfőbb problémát egy blokklánc alapú adatkezelésnél, ennek kivitelezésére is léteznek már - igaz, inkább kísérleti szinten - megoldások. Ezek szerint a törlést az adathoz való hozzáférés blokkolásával, ellehetetlenítésével lehet a gyakorlatban kivitelezni egy blokkláncban. Erre a vonatkozó irodalom az adathoz való hozzáférést biztosító privát kulcs törlését (elégetését) hozza megoldásként. A hozzáférési kulcs törlésével az adat megmarad a blokkláncban, azonban az ahhoz való hozzáférési/olvashatósági lehetőség a dekódoláshoz való kulcs hiányában végérvényesen elveszik. A kapcsolat megteremtéséhez való lehetőség végleges törlése tehát a GDPR szerinti „elfeledtetéshez való jog” érvényesítését szolgálhatja a blokkláncon.

Ezzel egybevágó vélemények szerint a megfelelő technológiával titkosított olyan személyes adatok, amelyekhez senkinek sincs hozzáférése, nem tartoznak többet a GDPR hatálya alá, kvázi elveszítik a rendelet által jelentett jogi garanciákra való érdemességüket. A titkosítási technológia elavulása és a potenciális újbóli hozzáférés veszélye azonban újraéleszti a jogi védelmet.
Egy másik lehetőség az ún. „felejtő” vagy „rövidített” blokkláncok koncepciója.

Egy ilyen alapon működő adatbázisban a hozzáférési kulcsokat tartalmazó blokkokat folyamatosan újrakalibrálják (hashelik) egy bizonyos, előre meghatározott idő után, így a hozzáférési lehetőség is elveszik. Ez tipikusan olyan célú adatkezeléseknél lehet jó megoldás, ahol az adatokat bizonyos idő után automatikusan törölni kellene.

Végül meg kell említeni a személyes adatok „láncon kívüli" („off-chain") tárolási lehetőségét, ahol a személyes adatokat nem magában a blokkláncban, hanem egy elkülönült adatbázisban tárolják, de kezelésük hash-kulcsok használatával összeköttetésben áll a háttértechnológiát adó alapadatbázissal, amely már blokklánc-alapon működik. A láncon kívüli adatokból való törléssel az alap blokklánc nem változik, csak az azzal összekötött, személyes adatokat is tartalmazó ráépülő adatbázis. Ezzel a megoldással kiküszöbölhető a blokklánc megváltoztatásának nehézsége és a személyes adatokat megillető védelem is érvényesül.

5. Összegzés

Mint láttuk a blokklánc egy rendkívül stabil adatkezelési megoldás, amely bármilyen személyes adat, információ kezelésére szolgálhat.

A technológia azonban működési alapelveit tekintve számos adatvédelmi kérdést felvet, amelyekre még nem léteznek megfelelően kiérlelt megoldások, habár azokkal folyamatosan kísérleteznek.

Fontos ezért, hogy az adatvédelmi megfelelés vizsgálata elsődleges legyen az olyan blokkláncok fejlesztésénél és tervezésénél, amelyek egyben személyes adatok kezelésére is szolgálnak, főleg ha okosszerződések megkötésére is használják azt. Az ilyen típusú, még nem kellően kiforrott, új technológiáknál ezért már előzetesen, annak használata előtt fontos elvégezni a GDPR által is előírt adatvédelmi hatásvizsgálatot.

Források:

-Bacon, J. et. al. (2017) Blockchain Demystified. Queen Mary School of Law Legal Studies Research Paper No. 268/2017
-Buterin V. (2013): A Next-Generation Smart Contract and Decentralized Application Platform. Online: https://ethereum.org/en/whitepaper
-Európai Központi Bank. (2017) How could new technology transform financial markets? 19th April 2017. Online: www.ecb.europa.eu/explainers/tell-me-more/html/distributed_ledger_technology.en.html
-Finck, M. (2019) Blockchain and the General Data Protection Regulation. European Parliamentary Research Service, PE 634.445.
-Giuseppe Ateniese - Bernardo Magri - Daniele Venturi - Ewerton Andrade: „Redactable Blockchain or Rewrtinig History in Bitcoin and Friends" in Proceeding of the 2nd IEEE European Symposium on Security and Privacy - EuroS&P 2017, eprint.iacr.org/2016/757.pdf
-Győrfi András et .al.: Kriptopénz ABC. Budapest, HVG Könyvek, 2019.
-Hossein Kakavand - Nicolette Sevres De Kost - Bart Chilton: The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies. SSRN Electronic Journal, (2017). Online: http://dx.doi.org/10.2139/ssrn.2849251
-Kachorowska, M. (2019) Blockchain-based land registration: Possibilities and challenges. Masaryk University Journal of Law and Technology, Vol. 13. No. 2. Online: https://doi.org/10.5817/MUJLT2019-2-8
-Nemzeti Adatvédelmi és Információszabadság Hatóság: Állásfoglalás a blokklánc („blockchain") technológia adatvédelmi összefüggéseivel kapcsolatban, Online: https://naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf
-Nick Szabo: „Smart Contracts: Building Blocks for Digital Markets" 1996 (részlegesen átdolgozva: 2018), www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf
-Rosanna Mannan - Rahul Sethuram - Lauryn Younge: „GDPR and Blockchain: A Compliance Approach" European Data Protection Law Review 3/2019.
-Schrepel, T. (2021): Smart Contracts and the Digital Single Market Through the Lens of "Law + Technology" Approach. European Commission. Online: https://ssrn.com/abstract=3947174
-Xing, B. és Marwala T. (2018): The Synergy of Blockchain and Artificial Intelligence. Online: http://dx.doi.org/10.2139/ssrn.3225357