Digital Trust Services adathitelesítő platform – blockchain alapú digitális ujjlenyomat tárolással

SOLYMOS GYULA
4iG Nyrt.
gyula.solymos@4ig.hu

Kulcszavak: blockchain, adathitelesség, Digital Trust Services, AI, felhőszolgáltatás, ZERO TRUST, ellátási lánc, termékkövetés, drón-feketedoboz

Az adatalapú gazdaságnak hiteles adatra van szüksége, amelynek a forrása, változatlansága igazolt, hogy arra alapozva kialakulhassanak a széleskörű adatalapú együttműködések, szak- és államigazgatás, valamint a másodlagos adatpiacok. Különös figyelmet kell fordítani az AI-megoldások betanító adatai hitelességének megvalósítására, mert csak így biztosítható ezen megoldások átlátható és biztonságos működése.
A blockchain-technológiára épülő Digital Trust Services egy digitálisujjlenyomat-alapú adathitelesítési platform megoldás, amely segítségével a digitális adatok széles körének hitelesítése és hitelességének ellenőrzése – iparág- és vállalkozásmérettől függetlenül – mindenki számára elérhetővé válik.

1. Bevezetés

A blockchain-technológiát sokan a kriptovalutákon keresztül ismerték meg és sokan még ma is azt gondolják, hogy egy energiafaló technológia, amit alapvetően a fintech világ szereplői tudnak kamatoztatni. Ezen a szemléleten ideje változtatni, hiszen *a blockchain a megbízhatóság technológiája,* amely segítségével elérhetjük, hogy egy adat hitelessége ne a jogszabályok betartásán és az adminisztráció megbízhatóságán múljon.

Napjainkban egyre több adatot állítunk elő és továbbítunk, és a formálódó adatalapú társadalomban egyre nagyobb az igény adatalapú együttműködésekre, ugyanakkor rengeteg hamisított adat vesz minket körül, ezért sokan elvesztették bizalmukat a digitális adatok iránt. Kétségtelenül egyre nagyobb veszélyt jelent a manipulált adat, amely előállítása a mesterséges intelligencia-megoldások használatával egyre könnyebb [1]. Miközben adatalapú társadalmat építünk, a manipulált adatok egyre nagyobb veszélyt jelentenek az adatalapú együttműködésekre és ellátási láncokra, adat-piacterekre, valamint a szak- és államigazgatásra is [2].

A cikkben bemutatásra kerül a *blockchain-technológiára épülő Digital Trust Services (DTS) platform megoldás,* amely megvalósításán az EU Important Projects of Common European Interest (IPCEI-CIS) programjában dolgozunk, és amely az új eIDAS reguláció tervezetre [3] alapozva képes lesz újraértelmezni a hagyományos adat fogalmát és megteremteni a *megbízható, ellenőrizhető adatalapú digitális ökoszisztéma* hátterét.

A DTS egyszerűségének és a jövőben szabad szoftverként elérhető digitális ujjlenyomatot előállító kódnak köszönhetően *nagyfokú interoperabilitást* fog biztosítani. Könnyen beépíthető lesz az adatgyűjtő szenzorokba és IoT-eszközökbe, valamint a kommunikációs és felhőmegoldásokba, így az adathitelesség automatikusan beépülhet minden cég és szervezet IT-megoldásába és így a mindennapi munkájába. A megoldás képes lesz a meglévő adatvagyon hitelesítésére, valamint a hiteles adatfelhasználás követésére is, amely az adatalapú együttműködések és adatpiacterek elterjedésének alapja lehet.

A cikkben röviden bemutatásra kerül egy általános célú fájlhitelesítő, valamint két ipari, egy agrár és egy egészségügyi területen fejlesztés alatt lévő laborinformatikai alkalmazáshoz kapcsolódó – a DTS pilotjának tekinthető – adathitelesítő blockchain-megoldás működése.

2. Adathitelesítési igény

Egyre több adatot termelünk a mindennapi tevékenységünk során, ugyanakkor azt tapasztaljuk, hogy ezekben az adatokban egyre kevésbé bízhatunk meg. Ennek oka, hogy egyre több olyan esetre derül fény, amikor akár globálisan is ismert cégek a publikált műszaki, termékminőségi, statisztikai adataikat a saját érdekeik szerint „kozmetikázzák” (pl. gépjármű CO2-kibocsájtása), vagy akár a termék származási, vagy gyártási adatait „zöldre mossák” [4]. További problémát jelent az egyre szaporodó IoT-eszközök száma [5], amelyek többnyire könnyen feltörhető kommunikációs csatornákon, illetve publikus internetes továbbítással közlekednek, és sokszor elsőként felhőmegoldásokban kerülnek letárolásra, így azok hitelessége és változatlansága sok szempontból megkérdőjelezhető [6].

A bizalmatlanságot tovább fokozza a rengeteg megtévesztésre alkalmas manipulált kép-, hang- és videóanyag, amivel nap mint nap találkozhatunk, és amelyek előállítása az interneten elérhető AI-alkalmazásokkal napról napra könnyebbé válik, így manapság ezen manipulációkat már nem csak a nagytudású szakemberek, hanem laikusok is meg tudják valósítani [7]. De nem csak képeket, videókat, hanem szinte mindenféle adatot egy-

re könnyebb észrevétlenül manipulálni, ideértve az IoT-szenzorok mérési, egészségügyi, diagnosztikai, GPS-követési, mezőgazdasági és egyéb adatokat is.

A manipulált adatokkal a hackerek könnyen összezavarhatják az együttműködő IT-rendszereket (például az energiaszektorban) anélkül, hogy bejutnának az adott cég tűzfalán belülre. *Növekvő veszélyt jelent a meglévő – akár éveken át gyűjtött – szakterületi (pl. egészségügy, agrárium), illetve szak- és államigazgatási adatbázisok manipulációja,* mert ha ezen adatok alapján hozunk döntéseket, vagy tanítunk be a jövőben AI-megoldásokat, akkor az nem az általunk elvárt eredményt, hanem a manipuláló érdekeit fogja erősíteni.

Képzeljük el, hogy mi történhetne, ha egy hacker hozzáférne az EU stratégiai adatbázisainak valamelyikéhez, és a saját érdekei szerint manipulálná azt, és mivel jelenleg nincs olyan megoldásunk, amivel meg tudnánk különböztetni a manipulált adatot a hitelestől, a következő naptól ezzel az adatbázisra alapozva végeznénk a munkánkat és hoznánk döntéseket.

Miközben digitális gazdaságot és társadalmat építünk, amiben egyre nagyobb szerepe van az adatoknak, a mindennapos és egyre könnyebb adatmanipuláció révén elveszett a bizalom a digitális adatokban! Ez a bizalomvesztés gátolja az adatalapú együttműködések, a másodlagos adathasználat és az adatpiaciok kialakulását is.

2.1. Az adathitelesség iránti igény legfőbb területei

Az adathitelesség igénye egyre erősebben jelenik meg az alábbi területeken:

- Adatvezérelt üzleti működés
- Digitális adatalapú együttműködések
- Termékkövetés
- Adatvezérelt közigazgatás
- V2X- és M2M-kommunikáció
- Adatpiacterek
- ZERO TRUST-alapú rendszerek [8]

2.2. AI/MI betanító adatok hitelességének kritikus fontossága

A gépi tanulási megoldásokhoz *nagy mennyiségű megbízható adatra van szükség,* mivel ezen rendszerek azok alapján tanulnak és fognak működni [9]. Amennyiben egy ilyen betanító adatbázisba nem az adott eljáráshoz tartozó, vagy véletlen, illetve sérült adatok kerülnek, úgy az MI-alapú megoldás hibásan fog működni.

Még jelentősebb problémát okozhat, ha az MI-megoldásokat rosszindulatúan (hackerek, vagy az adatokhoz hozzáférő belső emberek), valamely érdek szerint szisztematikusan manipulált adatokkal tanítják be [10]. Ezzel könnyen elérhető, hogy az AI/MI-alkalmazások észrevétlenül az érdekeknek megfelelően működjenek, például egy adott termék választását, vagy manipulatív üzleti döntést javasoljanak.

A gépi tanulási megoldások a betanítás után egyfajta fekete dobozként működnek és a hagyományos algoritmusokhoz hasonlóan a működésük taxatív módon nem ellenőrizhető, – ugyanakkor egyre kritikusabb döntések megalapozásához hívjuk őket segítségül –, ezért csak akkor bízhatunk meg bennük, ha biztosítjuk a betanító adatok hitelességét és manipuláció-mentességét, így ezek *ellenőrizhetőségének és hitelességének megteremtésére, valamint jogszabályi előírására is kritikusan nagy figyelmet kell fordítani*.

2.3. A digitális adat, mint termék hitelessége

A hackerek ma már nem csak eltulajdonítani, vagy blokkolni akarják az adathozzáférést, hanem egy annál sokkal veszélyesebb elkövetési mód; *az adatmanipuláció, mint hacker-módszer* kezd kibontakozni, ami azokra a cégekre jelent még nagyobb veszélyt, amelyeknek a terméke maga a digitális adat.

Egy tengerentúli egészségügyi szolgáltatót már ért a közelmúltban ilyen incidens, melynek során a támadók a több tízezer elért adatból csupán néhány tucat képalkotó diagnosztikai leletet manipuláltak AI segítségével, de mivel nem tudták ellenőrizni, melyik kép hiteles, vagy melyik hamis, kénytelenek voltak a hackerekkel megállapodni.

3. Adathitelesítés: Global State of the Art

Digitális dokumentumok hitelesítésére a cégek és az igazgatás szereplői jellemzően a „digitális aláírást" használják [11], amely bevett gyakorlat, de nem alkalmas az egyre nagyobb tömegben előállított olyan digitális adatok hitelesítésére és hitelességének ellenőrzésre, mint az IoT-adatok, szerverlogok vagy AI-betanításhoz használt adatok, illetve a meglévő adatbázisok, amelyeket a cégek meg szeretnének osztani egymással, vagy a formálódó adatpiacokon értékesíteni.

Vannak ugyan SSL- [12] és egyéb tanúsítványok az operációs rendszerekben és a böngészőkben, és sok helyen alkalmazzák a hash-képzési technológiát is [13], de ezek nem jelentenek egységes, mindenki számra elérhető olyan megoldást vagy eszközt, amelyekkel a felhasználó teljes bizonyossággal ellenőrizni tudná, hogy egy általa felhasznált adat a keletkezésétől, illetve a hitelesítéstől kezdődően változatlan.

A fentiek miatt egyre több cég keresi az adathitelesítés alternatív lehetőségeit, és egyre többen kezdik el használni a Blockchaint, mint hitelesítési technológiát. A ma épülő új adathitelesítési megoldások azonban teljesen zárt rendszerek, így csak egy-egy együttműködő cégháló igényeit képesek kielégíteni. Erre jó példa a PharmaLedger platform [14], amely a gyógyszeripar termékkövető és adatmegosztó megoldása, vagy – a Magyar Nemzeti Bank által indított – a Magyarországon működő bankok és biztosítók közt történő hiteles adatmegosztást biztosító blockchain-alapú rendszer. Mindkettő alapvetően egy zárt üzleti csoport igényei alapján lett kidolgozva, és nem alkalmas arra, hogy ez a két „siló" rendszer hitelesen osszon meg adatokat egymás közt, azaz abszurd módon nincs például lehetőség arra, hogy

egy gyógyszergyár a digitális adatait hitelesen megosszsza a bankjával, hiába van mindkettőnek adathitelesítést szolgáló megoldása.

Kijelenthető, hogy a technika mai állása szerint a cégek (ill. iparágak) egyedi, zárt adathitelesítési megoldásokat fejlesztenek, melyek egymás közt nem átjárhatóak, ami így gátolja az iparágakon átívelő adatalapú együttműködéseket, az adatpiacok kialakulását.

4. Blockchain-adathitelesítés és problémái

A blockchain-adathitelesítés az adatok összeláncolásán túl a blockchain „validátor" csomóponti szerverek konszenzus mechanizmusára épít. Ennek következtében a láncba írt adatok minden csomóponti szerverhez hozzáférő szervezet, illetve annak felhasználója által elérhetővé válnak, amely üzleti alkalmazás esetén több kérdést is felvet.

Publikus blockchain-hitelesítés

Egy adat vagy dokumentum hitelességét úgy biztosíthatjuk a legegyszerűbben, ha azt egy publikus blockchain-láncra (pl. Ethereum [15]) feltöltjük. Ez az adat bármikor később kiolvasható a publikus blockchainből, és mivel a működéséből adódóan az nem megváltoztatható, ezért biztosak lehetünk benne, hogy a letöltéskor a feltöltött adat vagy dokumentum azonos lesz a feltöltött anyaggal.

Mivel azonban a publikus blokkláncok teljes tartalmát minden validátor-csomópont (akár több százezer ismeretlen szereplő) eléri, azok üzleti adatok kezelésére csak erősen korlátozottan használhatóak, mivel az adott adat vagy dokumentum „mindenki" számára elérhetően jelenik meg.

A publikus láncok további korlátja, hogy azok működésének díjfizetése az adott lánc saját fizetőeszközéhez kötött (Ether, Bitcoin stb.), így ezen rendszerek használatának nagy a pénzügyi kitettsége és volatilitása. További probléma, hogy a különösen a kisebb láncok esetében a gyakorlatban nem elképzelhetetlen a validátorok 51%-os rosszindulatú összejátszása, ami pont a tárolt adatok integritásába vethető bizalmat kérdőjelezi meg.

Enterprise, „zárt" blockchain és az adattárolás problémája

A publikus blokkláncok korlátozott üzleti felhasználhatóságát az enterprise blokkláncmegoldások segítségével kiküszöbölhetjük azáltal, hogy egy ilyen megoldásban *minden validátor-csomópontot üzemeltető szereplő ismert*. Ezt a megoldást előszeretettel használják az azonos iparágban együttműködő cégek és ellátási láncok a termékeikhez kapcsolódó digitális adatcseréjük hitelesítésére (pl. PharmaLedger).

Amíg egy termékhez tartozó adatot hitelesítünk és osztunk meg másokkal, addig ez a megoldás kiválóan működik, viszont, ha egy olyan rendszert szeretnénk felépíteni, amiben konkurens cégek, illetve üzleti szereplők, vagy azokat felügyelő szervezetek is részt vesznek, és *nem szeretnénk, hogy a hitelesítő csomópontot futtató szervezetek láthassák mindenki blokkláncba feltöltött üzleti adatát, akkor elértük ezen megoldások korlátját.*

Természetesen titkosítva is feltölthetjük a blokkláncba az adatokat, de annak kezelése jelentősen megnöveli a kiépítendő rendszerünk komplexitását, erőforrásigényét, árát, és nem utolsó sorban jelentősen lassítani fogja annak működését.

Szintén problémát jelent, hogy az együttműködő cégek iparáganként egyedi adattárolási metódusokat és megoldásokat fejlesztenek. Ezekben hiába vannak blockchain-megoldásra építve hitelesen tárolva az adatok, ha egy másik iparág vagy a rendszerhez csatlakozó külső szereplő számára egy adott adat hitelessége nem igazolható. *Ezek a rendszerek ezért csak siló-szerűen, más iparágak vagy szereplők felé történő interoperábilitás lehetősége nélkül működnek.*

5. Digital Tust Services (DTS) platform és működése

5.1. A DTS célja és eredménye

A DTS célja olyan *blockchain-technológiára épülő, iparágtól és adattípustól független, interoperábilis hitelesítő és hitelességellenőrző felhőszolgáltatás létrehozása,* amely megteremti az adatok tömeges hitelesítésének platformját.

A projekt fő célja az adatok (IoT, szenzor, kép, videó stb.) keletkezésekor, illetve első kommunikációs csatornákba kerülésekor történő azonnali hitelesítése, de a megoldásunk lehetőséget biztosít a már meglévő adatvagyon és speciális adatok (pl. security, programkód) hitelesítésére is, megteremtve ezzel a hiteles adatok hasznosítására, illetve egymás elektronikus dokumentumainak elfogadására épülő együttműködéseket, valamint az adatcsere és az adathozzáférések hiteles visszakövethetőségét is.

A projekt eredményeként egy olyan, több országban is alkalmazható adathitelesítési platform jön létre, amely alkalmas nagymennyiségű adat hitelesítésére és annak felhasználása előtti hitelesség, változatlanság és teljeskörűség ellenőrzésére. A platformhoz, annak interfészei segítségével, bármely meglévő szoftvermegoldás csatlakozható, így annak hitelesítése a meglévő iparági és közigazgatási, valamint adatcsere- és piactér-alkalmazásokba is könnyen beépíthető lesz.

A blockchain- (distributed ledger) technológia hitelessége az EU elektronikus azonosításról és bizalmi szolgáltatásokról szóló *eIDAS 2.0 rendeletének* új szövegtervében is szerepel, így annak hitelessége magas szinten is elismert, ami a *DTS-megoldás jogi hátterét* biztosítja.

Projektünk célja, hogy az Európai Uniós megbízható adatterek kialakítását és adatfelhasználási regulációk és célok elérését támogassa a *GAIA-X, Data Governance Act, AI Act, EU Trust Mark, New Industrial Startegy, SME Strategy* törekvésekhez illeszkedve.

5.2. A DTS működésének rövid műszaki összefoglalása

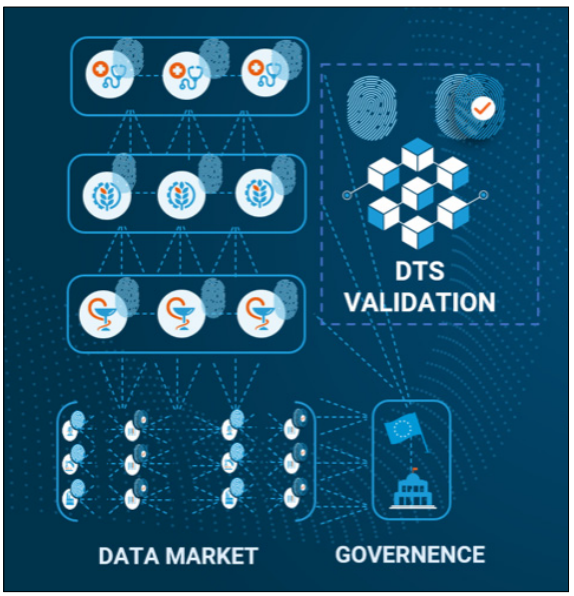
A DTS-platform adathitelesítése (ideértve a dokumentumokat, média- és egyéb elektronikus anyagokat is) az adatok digitális ujjlenyomatának, avagy #HASH-értékének előállításán és egy olyan zárt, enterprise blockchain megoldást alkalmazó tárolásán alapul, amely hitelesítő szervezetek által üzemeltetett független csomópontszerverek elosztott adattárolásával *szavatolja a hitelesítő #HASH megváltoztathatatlan tárolását és hiteles visszakereshetőségét.*

A #HASH egy olyan kriptográfiai módszerekkel előállított digitális leképezése az adatrekordnak, dokumentumnak, vagy bármilyen fájl tartalmának, amely az eredeti adat birtokában bármikor megismételhető, de ha az eredeti adat tartalmában a legkisebb módosulás is történt (például a dokumentumba belekerült egy „.") annak értéke már nem fog megegyezni az eredetivel. A #HASH ugyan a nyers adatból készül, de abból az adat maga semmilyen formában nem rekonstruálható.

A DTS-rendszerhez csatlakozók egy egységes #HASH MAKER modult kapnak, amelyet a saját hálózatukon belül telepítenek, és interfészek segítségével az adatgyűjtő, illetve kezelő megoldásaikkal összekapcsolnak, így az adatok hitelesítése (annak beállításainak megfelelően) automatikusan meg tud valósulni. A hitelesítő modulon az adat áthalad, de *a DTS-platform számára kizárólag csak a #HASH értékek és annak metaadatai (partnerazonosító, időbélyeg stb.) kerülnek továbbításra,* így a cég adatai házon belül maradnak.

Ezen működésnek köszönhetően a megoldás megfelel a GDPR követelményeinek, amely így számos üzleti területnek megoldást jelenthet, ahol most ezen szabályok betartása nehézségbe ütközik.

A digitális ujjlenyomat ugyan a már ismert megoldásra épül, de nem egy egyszerű #HASH, hanem egy olyan innovatív megoldás, ami a metaadatok segítségével *az adott adattípushoz tartozó egyedi munkafolyamait és üzleti elszámolási funkciókat is ki tudja szolgálni,* ugyanakkor nagyfokú interoperábilitást biztosít a különféle iparágak és ellátási láncok között.



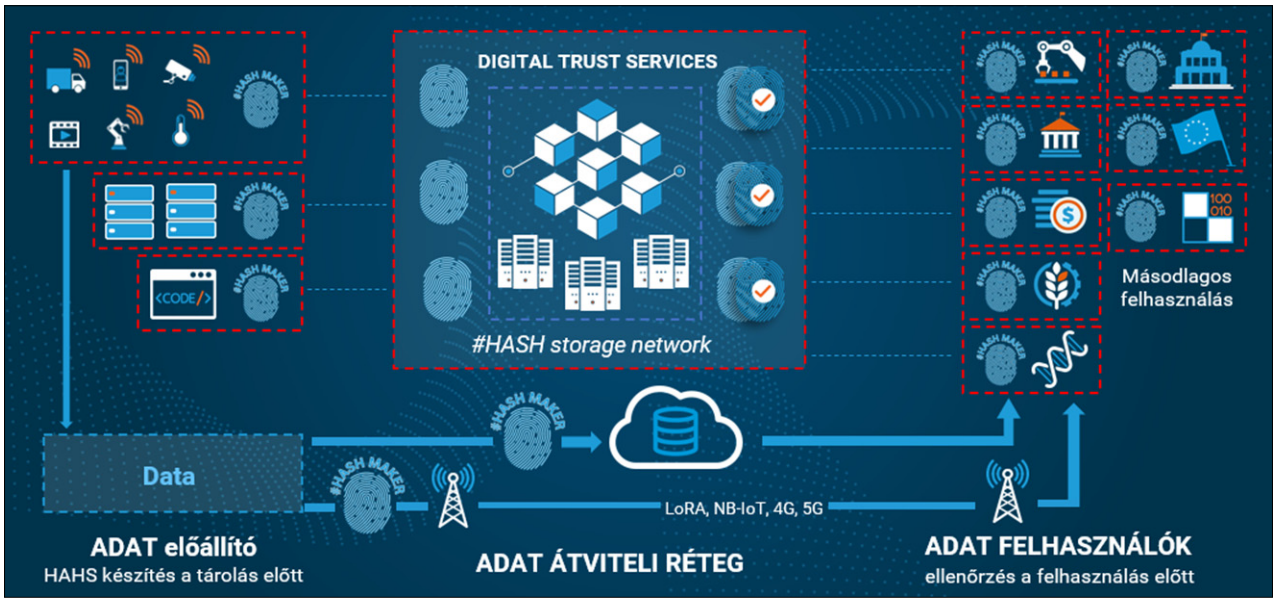
Amennyiben az adatujjlenyomat-előállítás az adatot előállító eszközben nem biztosítható, úgy a #HASH-képzés az azokat továbbító (pl. 5G, NB-IOT, LoRaWan műhold stb.) szolgáltató hálózatába érkezve – egyfajta értéknövelt szolgáltatásként – abba beépítve valósítható meg.

A felhőszolgáltatók szintén integrálhatják a #HASH MAKER megoldást a rendszereikbe, amely segítségével a felhőben tárolt, majd onnan felhasznált adatok változatlanságát az ügyfeleik ellenőrizni tudják, ezzel *növelve a bizalmat a felhőalapú tárolási megoldásokban.* A rendszer ugyancsak alkalmas a ZERO TURST elvárás szerint a felhőben és platformokon futó szoftvermegoldások és AI-algoritmusok kódjainak módosítás- és manipulálás-mentességét igazolni, ami napjainkban egyre fontosabb.

ADATMEGOSZTÁS – HITELESSÉGELLENŐRZÉS

Az adatgazda az adatot továbbra is a megszokott módon (direkt kapcsolat, API, e-mail stb.) oszthatja meg a partnereivel vagy harmadik féllel, akik a megkapott adatról a DTS #HASH MAKER megoldása segítségével előállítják annak digitális ujjlenyomatát. Ennek DTS-rendszerbe történő beküldésével és ellenőrzésével *az adatot fogadó partner, üzleti, vagy közigazgatási szereplő ellenőrizni tudja az adat tartalmának sértetlenségét, teljeskörűségét, a hitelesítés keletkezésének időpontját, illetve az azt előállító entitás (természetes/jogi személy vagy eszköz) adatait is.*

Mivel a *DTS #HASH MAKER szabad szoftverként elérhető megoldás* lesz, így annak kódját bárki elérheti, beépítheti a meglévő alkalmazásába, weboldalába, szolgáltatásába, vagy végfelhasználóként applikációként letöltheti és így könnyen ellenőrizheti bármely általa (levélben, weboldalon, interfész stb. keresztül) megkapott adat, kép, dokumentum stb. hitelességét és változatlanságát.



DTS – Hitelesítés- és hitelesség-ellenőrzés digitális ujjlenyomat segítségével

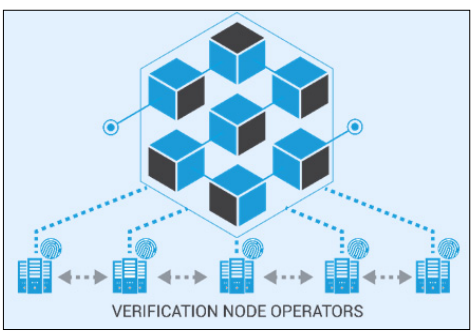
Amennyiben az adattulajdonos az *adat-nyomkövetési funkciót* is bekapcsolja, úgy a DTS-platform blockchain-okosszerződés (smart contract) segítségével egyedileg engedélyezi/tiltja az adathitelesség ellenőrizhetőségét, így a rendszerünk az illetéktelenül megszerzett adatok hitelesként való felhasználását meg tudja akadályozni. Mivel ez esetben a DTS logolja a hitelesség ellenőrzők azonosítóit, így az adathasználók köre is visszakövethetővé válik.

Az európai országokon átívelő együttműködésekben érintett adatok megosztásakor azok digitális ujjlenyomatát (#HASHértékeket) az érintett országok DTS-platformjai mellett az *EBSI Európai Blockchain Szolgáltatásban* is tervezzük letárolni, illetve hitelesíteni.

5.3. Többcsatornás adathitelesítés – az igényekre szabott bizalom garanciája

A blockchain-rendszer az adatok összeláncolásán túl, azok hitelességét a DLT (Distributed Ledger Technology), az elosztott főkönyvi rendszer [16] garantálja. Ezen főkönyvek – azaz a DTS-blockchainben tárolt digitális ujjlenyomatok a verifikációs node-ot üzemeltetők szerverein is megjelennek.

A hitelesség konszenzusos igazolásához azonban minimálisan elegendő egy lánc három csomóponton való tárolása. Erre építve a DTS egy úgynevezett többcsatornás adathitelesítési modellt épít fel, ahol az *egyes iparágak vagy együttműködő szereplők maguk választhatják ki és dönthetik el, hogy mely szereplők futtassák közülük a hitelesítésben résztvevő csomóponti szervereket.* Ezáltal egy ellátási láncban nem szükséges minden szereplőnek validációs csomópontot fenntartania, elég, ha azon szereplők közül három üzemeltet ilyen szervert, akikben a többiek megbíznak.



A hitelesítő szereplők ugyanakkor nem csak az adatelőállításban résztvevő szereplők lehetnek, hanem akár közigazgatási, kamarai, minisztériumi szervezetek is, akit maga az iparág vagy az állam nominál a feladatra. Fontos ugyanakkor ismételten megerősíteni, hogy mivel a DTS adatujjlenyomat-alapú működéséből következően nem kerül adat a blockchainba, így *a hitelesítésben résztvevő szereplők csak az adathoz tartozó #HASH- és metaadatokat tárolják, magát az adatot nem!*

Annak, hogy a DTS-ben a hitelesítés csatornákra osztható, a legfőbb előnye, hogy minden csatorna a szereplői által megbízhatónak ítélt szereplőkkel validáltathatja az adatot. A hitelesítő szereplők közt átfedések is lehetnek, azaz lehet olyan szereplő, aki több csatorna hitelesítési konszenzusában is részt vesz. Ilyenek lehetnek a fent is említett állami, kamarai, vagy szakigazgatási szereplők, amelynek köszönhetően a hitelesített adatokat *az állami folyamatokban is elfogadják, ami az adatalapú közigazgatás megteremtésének alapfeltétele.*

5.4. Alkalmazási példák

- IoT- és szenzoros adatgyűjtés adatainak hitelesítése.
- Ipar 4.0 során keletkező adatok hitelesítése – megbízható minőségi és műszaki adatok/garancia.
- Logisztikai folyamatok, termék- és járműkövetés, átadás-átvétel, felhasználáshitelesítés.
- Élelmiszer-előállítás (vegyszerhasználat, származás) adatainak hitelesítése.
- Egészségügyi adatok, leletek, képi diagnosztika hitelesítése/manipulációmentesség igazolása.

- Laborfolyamatok (humán, állatorvosi, élelmiszer, ipar) minőségbiztosítása.
- Energetika: Smart Grid/okos mérők és elszámolások hitelesítése.
- Ügyvitel digitális aláírás nélkül: dokumentumok, fájlok tartalmi hitelesítése és továbbítása, átvételkövetés.
- Médiaanyagok (hangrögzítés, videó, kép, hírforrás stb.) hitelesítése.
- IT Security: LOG-hitelesítés, router konfiguráció ellenőrzés, szoftverkód-hitelesítés stb.
- Mesterségesintelligencia-betanító adatok hitelesítése.
- XML adatok, alkalmazások közti adatcsere érkezés- és fogadáshitelesítés.
- Adatalapú jogügyletek és szakigazgatási bevallások alapjának megteremtése.
- EU Green Deal/ESG célok adatalapú bevallása/ellenőrzése.

A fent felsoroltak csak példák az alkalmazhatóságra, ezen felül számos további üzleti és közigazgatási alkalmazási terület azonosítható és valósítható meg.

5.5. Adathitelesítési pilotprojektek rövid bemutatása

Az alábbiakban olyan projekteket szeretnék röviden bemutatni, amelyek mögött a DTS-koncepciót alkalmazó pilotmegoldás működik, vagy hamarosan működni fog.

5.5.1. Ipari termék minőségellenőrzése

A Széchenyi Egyetemmel karöltve egy egészségügyi implantátumokat gyártó cégnél egy gépilátás-alapú ipari termék minőségét ellenőrző rendszer került kidolgozásra. A termékek minőségét igazoló adatok hitelesítésére a DTS digitális ujjlenyomat-alapú megoldásának pilotváltozatát építettük be, amely az alábbi adatokat hitelesíti:

- Kamera által készített tárgykép (egyedi azonosítószám felismeréssel),
  - gyártási hely, operátor, anyag származása stb.
- Gépitanulás-alapú gépilátás-szoftvermegoldás verzió és minőségellenőrzési paraméterek.
- A gépilátás-megoldás által feldolgozott eredménykép, minőségi adatok,
  - nem megfelelő minőség esetén a javítás, korrekció utáni újabb adatok összefűzése.

A projekt eredménye: *a gyártó termékeinek minőségét a nemzetközi forgalmazók, az azt felhasználó kórházak, illetve maguk a betegek is leellenőrizhetik* egy, a termékről – akár egyszerű e-mailben megküldött – a minőségellenőrzés során készített fénykép és minőségi bizonyítvány alapján. Mivel ezen dokumentumok a DTS-sel hitelesítettek, azok digitális ujjlenyomatának ellenőrzésével azok eredetisége, manipulációmentessége könnyen leellenőrizhető.

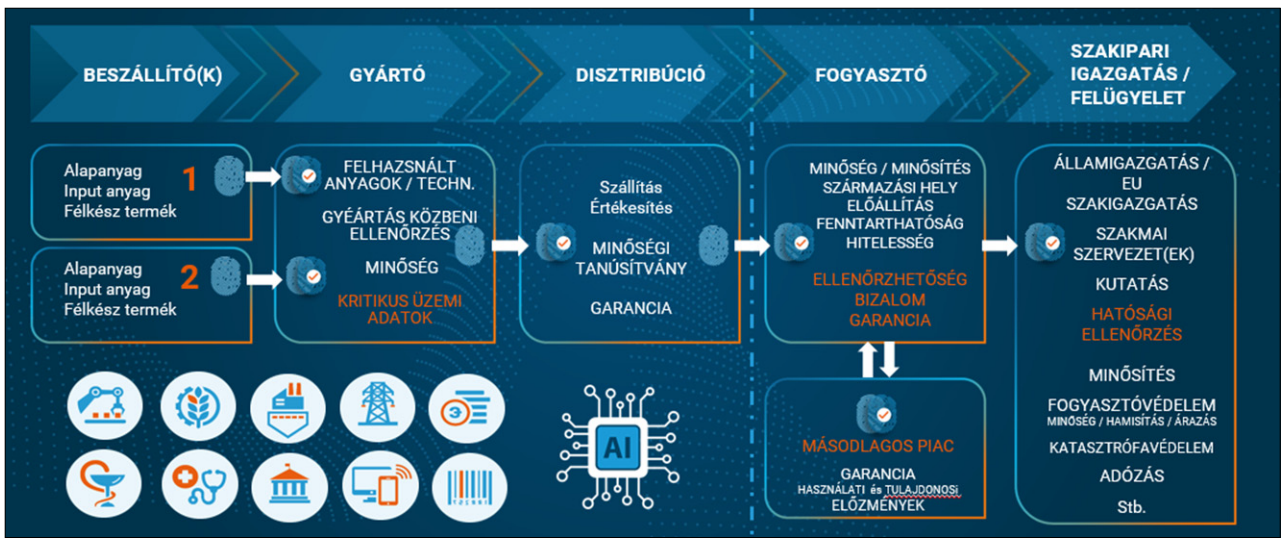
5.5.2. Ipari karbantartási és szerviztevékenység hitelesítése

A Széchenyi Egyetemmel együttműködve egy egészségügyi implantátumokat gyártó cégnél megvalósuló 3D/VR „Digital Twin" megoldás részeként elkészülő karbantartást támogató és tevékenységet naplózó rendszerbe integrálásra kerül a DTS digitálisujjlenyomat-alapú megoldásának pilotváltozata, amely az alábbi adatokat hitelesíti:

- Karbantartási/szerviztevékenység naplóbejegyzései:
  - munkavégző személy(ek),
  - tevékenység megnevezése, leírása,
  - felhasznált/kicserélt alkatrészek/kellékanyagok listája.
- Karbantartást/kellékanyagcserét igazoló fénykép, jegyzőkönyv, dokumentáció.

A projekt eredménye: *létrejön egy hiteles adatokra épített karbantartási és szerviztevékenységet naplózó megoldás.* Az ebben tárolt adatokban minden érdekelt szereplő, a gépszállítótól kezdve a karbantartásért felelős és a cégvezetők is megbízhatnak. A hiteles karbantartási/igazolt minőségű kellékanyag használati adatokra garanciaérvényesítési és üzemeltetésellenőrzési/karbantartási felhasználási esetek építhetőek.

Adathitelesség biztosítása a teljes ellátási láncban



5.5.3. Drónrepülési és permetezési feketedoboz (flight recorder)

A drónhasználat és a permetezés (azaz vegyszerkijuttatás) veszélyes üzem, azért a drón repülését és a permetlé elsodródását okozó meteorológiai körülmények hiteles igazolása a drónhasználat elterjedésével egyre fontosabb megoldandó kérdés.

A projekt során kidolgozott, a szél elsodródási hatását a drón útvonalának folyamatos módosításával kompenzáló Precíziós Drón Permetezési Platform háttérszolgáltatásaként beillesztettük a DTS pilotverzióját, amely *a drón repülési, telemetriai és permetezési munkavégzési (szemcseméret, nyomás, vegyszer stb.), valamint időjárási adatait digitális ujjlenyomat technikával hitelesíti.*

A projekt eredménye: a platform háttérszolgáltatásaként egy *drónrepülési feketedoboz jön létre,* amely segítségével vitás esetekben a drón útvonala és a kijutatott vegyszer, a repülés során mért meteorológiai adatok – és az abból következő vegyszer-elsodródás és -kompenzáció adatai – *hitelesen kinyerhetőek és vizualizálhatóak.* A pilotprojekt hosszú távon egy általános célú, minden – nem hobbi-, illetve afeletti kategóriájú – drón repülési adatát hitelesítő, a polgári repülésben használt megoldáshoz hasonlóan hiteles feketedoboz-megoldás megalapozását is hivatott előkészíteni.

5.5.4. #HASH – Fájlhitelesítő és hitelességellenőrző megoldás

#HASH munkanéven elkészítettünk egy webböngészőben elérhető pilotszolgáltatást, amelynek célja, hogy bármilyen fájl (word, xls, kép, videó stb.) egyszerű módon hitelesíthető legyen. A hitelesítő felhasználó által feltöltött fájlokról (a megadott metaadatokkal kiegészítve) a megoldásunk elkészíti annak „digitális ujjlenyomatát", és elküldi a DTS blockchain-hitelesítő rendszer számára.

A felhasználó a hitelesített fájlokat *bármilyen szokványos (email, felhő, social platformok, chat pendrive stb.) módon megoszthatja a partner(ei)vel.* Ezen partnerek a #HASH-szolgáltatás felületére hitelességellenőrző felhasználóként belépve, a megkapott fájlok feltöltésével, annak digitális ujjlenyomatának elkészítésével és blockchainben tárolt változatával történő összehasonlításával ellenőrizheti a fájlok hitelességét és változatlanságát.

Amennyiben a fájl hiteles, a rendszer a fájlhoz tartozó metaadatokat is kiírja az ellenőrző felhasználó számára, így az meggyőződhet róla, hogy a fájlt, dokumentumot mikor és ki hitelesítette, azóta változott-e annak verziója, illetve (például termék esetén) milyen további kapcsolódó (garancia, minőségellenőrzés stb.) dokumentumok állnak rendelkezésre.

A projekt eredménye: egy olyan webböngésző-alapú, a DTS működési elvéhez igazodó megoldás, amely fájltípustól függetlenül képes előállítani azok digitális ujjlenyomatát, ami alapján az adott fájl (annak ismételt feltöltésével) annak változatlansága és metaadatai (hitelesítő szervezet, felhasználó, időpont stb.) is ellenőrizhetővé válik. *A megoldás kizárólag csak a digitális ujjlenyomat előállításának erejéig futtatja át a fájlt a rendszeren, azaz semmilyen formában nem tárolja azt.*

5.5.5. Laborinformatikai munkafolyamat követés

Egy K+F projekt keretében kifejlesztett orvosi célú laborinformatikai szoftvermegoldás munkafolyamat- és adatkezelő rendszerében tárolt adatok hitelesítésére tervezzük a DTS-megoldásunkat beépíteni.

Ennek segítségével egy olyan egyedülállóan hiteles adatokra építő, a laborfolyamatokat hitelesítő megoldás jön létre, amely hitelesíti a következőket:

- A labor-mintavételezés helye, a mintavevő személye, végzettsége.
- A laborminta szállításának átadás-átvétele, szállítási körülmények.
- A labormintát feldolgozó laboráns felhasználó azonosítása, végzettsége.
- *Minden, a laborálás során történő mintatovábbítás, átadás-átvétel munkafolyamat és személy hitelesítése.*
- Laboráló gép működési adatai: kalibrálás, kötelező karbantartás, reagenshasználat.
- Laborkiértékelést hitelesítő azonosítása, végzettsége.
- Kiállított laboreredmény-dokumentum hitelesítése,
  – a hitelesítéshez kapcsolódóan a háttérfolyamatok hitelessége is igazolható.

Elvárt eredmény: A laborálás, az ahhoz használt gépi erőforrások pontossága, hitelessége, az emberi erőforrások szakértelme és az annak eredményeképpen álló lelet hitelessége igazolható a teljes labor mentén. A felhasználó, a folyamatban érintett személyek azonosságát és megfelelő diplomával való rendelkezését hosszabb távon az EBSI (European Blockchain Sevices Infrastructure) megvalósító megoldásai által szeretnénk ellenőrizhetővé és igazolhatóvá tenni.

6. Összefoglalás

A digitális adatalapú gazdaság és közigazgatás hatalmas előnyt nyújt az üzleti és a civil szereplők számára is, ugyanakkor a nem hiteles adatokra épített adatalapú együttműködések, adatpiacok, szakértői, illetve mesterséges intelligencia- és gépi tanulási megoldások kritikus biztonsági kockázatot jelentenek a teljes társadalomra nézve.

Ennek kivédésére a digitális gazdaság működésének alapját *az ADAT-ot a keletkezési helyéhez lehető legközelebb hitelesíteni kell,* amihez létre kell hozni egy olyan infrastruktúrát, amely iparágtól és cég méretétől függetlenül elérhetővé teszi az adatok tömeges hitelesítését, valamint annak interoperábilis ellenőrzésének lehetőségét.

Az adathitelesítésre a blockchain-technológia alkalmazása olyan megoldást kínál, ahol a hitelességet nem a jogszabályok betartása, vagy a rendszergazdákban való bizalom, hanem maga a technológia és az abban tárolt adatok megváltoztathatatlansága garantálja.

A cikkben bemutatott Digital Trust Services (DTS) megoldás többcsatornás hitelesítő csomópont felépítését biztosítja, hogy az adathitelességet olyan szereplők konszenzusa biztosítsa, akikben az adathitelesítők maguk megbíznak. A hitelesítésben szerepet vállalhat a szak- és államigazgatás is, annak érdekében, hogy az adat az adatalapú kormányzás során is felhasználható legyen.

A hiteles, ellenőrizhető adat létrejötte erősíti a bizalmat a teljes ellátási láncban, a vásárlókban és az igazgatási szereplőkben, míg annak ZERO TURST-megközelítéses alkalmazása jelentősen megnehezíti a hackerek és az adatmanipuláció lehetőségeit.

Nagyon fontos, hogy *a cégek a lehető leghamarabb elkezdjék beépíteni adatgyűjtési és feldolgozási megoldásaikba az ADATHITELESSÉGET,* mert ma még ez csak extra igénynek tűnik, de hamarosan már alapelvárás lesz a fogyasztóktól, és akinek nem lesz hiteles adata a termékéről, illetve annak előállításáról, az lemarad a versenyben a nemzetközi cégek mögött! *Ez különösen fontos azon cégek esetében, akiknek a terméke valamilyen digitálisan tárolt adat (pl. CT-felvétel), vagy AI/Ml-megoldás,* mert ha nem tudja igazolni ezek hátterében lévő adatok hitelességét és manipulációmentességét, akkor rövidesen nem fogja tudni értékesíteni a terméket, illetve megoldást.

Ha megteremtjük a megbízható adat fogalmát, tovább léphetünk a blockchain következő lehetőségének kiaknázásához: az aláírás nélkül is hiteles, automatikusan teljesülő *Digitális Szerződések (Smart Contract) és Token gazdaság* irányába, ugyanakkor az ebben rejlő lehetőségek kiaknázásához a jogszabályi háttér hazai kidolgozása is szükséges.

A DTS-projekt az Európai Unió IPCEI-CIS programjában megvalósítani kívánt rendszerként jelentős szerepet kíván vállalni a hiteles adatokra épített Európai Cloud ökoszisztéma hiteles adatokra való építésében és működésében.

Hivatkozások

[1] A. Chadha, V. Kumar, S. Kashyap, and M. Gupta, "Deepfake: An Overview", in Proc. of 2nd International Conf. on Computing, Communications and Cyber-Security, P.K. Singh, S.T. Wierzchoń, S. Tanwar, M. Ganzha, and J.J.P.C. Rodrigues, Ed., in Lecture Notes in Networks and Systems. Singapore: Springer, pp.557–566., 2021. doi: 10.1007/978-981-16-0733-2_39.

[2] P.B.K. Payne and P.H. Wu, ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited, 2020.

[3] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity", *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN*

[4] M. Lukinovic and L. Jovanovic, "Greenwashing – fake green/environmental marketing", Fundamental and applied researches in practice of leading scientific schools, Vol. 33, pp.15–17., 2019. doi: 10.33531/farplss.2019.3.04.

[5] A. Castillo és A. Thierer, "Economic Perspectives Projecting the Growth and Economic Impact of the Internet os Things", 2015. doi: 10.2139/ssrn.2618794.

[6] M. Sain, Y.J. Kang, and H.J. Lee, "Survey on security in Internet of Things: State of the art and challenges", in 19th International Conf. on Advanced Communication Technology (ICACT), pp.699–704., 2017. doi: 10.23919/ICACT.2017.7890183.

[7] S. Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes", IEEE Transactions on Technology and Society, Vol. 1., nr.3, pp.138–147., 2020. doi: 10.1109/TTS.2020.3001312.

[8] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture", National Institute of Standards and Technology (NIST), Special Publication, 800-207, 2020. doi: 10.6028/NIST.SP.800-207.

[9] Z. Ghahramani, "Probabilistic machine learning and artificial intelligence", Nature, Vol. 521., nr.7553., 2015. doi: 10.1038/nature14541.

[10] M.A. Ramirez et al., "Poisoning Attacks and Defenses on Artificial Intelligence: A Survey", arXiv, 2022. doi: 10.48550/arXiv.2202.10276.

[11] J. Katz, "Digital Signatures", Boston, MA: Springer US, 2010. doi: 10.1007/978-0-387-27712-7.

[12] "The SSL Protocol". *http://www.webstart.com/jed/papers/HRM/references/ssl.html*

[13] B. Preneel, "Cryptographic hash functions", European Transactions on Telecommunications, Vol. 5, nr.4., pp.431–448., 1994. doi: 10.1002/ett.4460050406.

[14] Pharmaledger, online: *https://pharmaledger.eu/*

[15] D.G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger", *https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf*

[16] M. Rauchs et al., "Distributed Ledger Technology Systems: A Conceptual Framework". Rochester, NY, 2018. doi: 10.2139/ssrn.3230013.

A szerzőről

SOLYMOS GYULA villamosmérnök, vállalkozás és minőségbiztosítási szakdiplomás menedzser. Több mint 20 éve dolgozik az IT világában, ahol széleskörű tapasztalatot szerzett a modern technológiákra épülő innovatív megoldások fejlesztésében. 2019-ben csatlakozott a 4iG Nyrt.-hez, ahol mesterségesintelligencia-, 5G-, és blockchain-technológia-alapú megoldásokkal és üzletfejlesztési projektekkel foglalkozik. Fő célja, hogy az innovatív ötletekből valós üzleti problémákra választ adó megoldásokat kovácsoljon. Közel 3 éve foglalkozik a blockchain-technológiával, amely alkalmazásáról már számtalan előadást tartott. A 2022 márciusában megalakult a Blockchain Koalíció Ellátási Lánc munkacsoportjának vezetőjeként célja, hogy a technológia szerepét minél több iparágban megtalálja és ezáltal a hazai ökoszisztéma kialakulását és új alkalmazások megvalósulását katalizálja. A DTS platform ötlet- és projektgazdája, amit az Európai Unió számára is bemutatott és jelenleg annak Important Projects of Common European Interest (IPCEI-CIS) program keretében történő megvalósításának előkészítésén dolgozik.