BLOCKCHAIN-BASED IMPLEMENTATION FOR AUTOMOTIVE ENVIROMENT

BLOKKLÁNC ALAPÚ ALKALMAZÁS AUTÓMOBIL KÖRNYEZETRE[1]

NAGY Csaba Norbert[2] – OLÁH Norbert[3]

Abstract

Nowadays, the rapid development of the automotive industry poses new challenges for IT security and data management in vehicles. Numerous incidents (e.g. Kia and Tesla incidents) show the vulnerability of the vehicles. In our proposed solution, we have studied the automotive environment's characteristics, security features and requirements. We have designed a solution to enhance cyber resilience by using blockchain for secure identity and access management (permissioned blockchain, two-factor authentication) and distributed storage to store and manage data. Updating the software in cars is a critical point from the information security perspective. Our proposed implementation will alert the user of the release of new software updates (Over-the-Air), and the system components allow continuous updating of vehicle data, moreover, storage and validation of the user account password using smart contracts.

Keywords

IT security, Blockchain, Password management, Automative industry, Smart contracts

Absztrakt

Az autóipar gyors fejlődése új kihívásokat vet fel a járművek informatikai biztonságával és adatkezelésével kapcsolatban. Számos incidens mutatja az alkalmazott rendszerek sérülékenységét. Az általunk javasolt megoldásban az autómobil környezet jellemzőit, biztonsági sajátosságait és követelményeit tanulmányoztunk. Megoldást dolgoztunk ki a kiber-ellenálló képesség növelésére, amelyben blokklánc alkalmazásával biztonságos identitás- és hozzáférés-kezelést (engedélyköteles blokklánc, kétfaktoros hitelesítés) és elosztott tárolást dolgoztunk ki az adatok tárolása, kezelése érdekében. Az autók szoftvereinek frissítése kritikus pont információbiztonsági szempontból. Az általunk javasolt alkalmazás figyelmezteti a felhasználót az új szoftver frissítések megjelenéséről (Over-the-Air), a rendszer komponensei lehetővé teszik a gépjárművek adatainak folyamatos frissítését, továbbá a felhasználói fiók jelszavának tárolását és ellenőrzését okosszerződések alkalmazásával.

Kulcsszavak

IT Biztonság, Blokklánc, Jelszó menedzsment, Járműipar, Okosszerződések

[1] Jelen tanulmány az I. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián, 2023.10.25-én elhangzott előadás szerkesztett változata.

[2] nagy.csaba@inf.unideb.hu | ORCID: 0009-0009-0678-281X | technician, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| technikus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

[3] olah.norbert@inf.unideb.hu |ORCID: 0000-0002-0007-8508| Assistant Professor, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| adjunktus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

BEVEZETÉS

Az autóipar digitalizációjának eredményeként a modern járművekben megjelenő különböző hardverekből és szoftverekből álló rendszerek számos egyezést mutatnak a dolgok internetének (IoT) rendszereivel mind felépítésben, mind működésben és az ezeket a rendszereket érő kihívásokban egyaránt. A járműipari digitalizáció így nem csak új lehetőségeket hozott magával, hanem új problémákat és felelősségeket is a gyártók és felhasználók számára. A járművek egyre komplexebbé válnak, amelyek a hétköznapi életünk központi részévé váltak a közlekedésben és a szállításban. Ahogy a hagyományos informatikai rendszerek és szoftverek is rendszeres frissítéseket igényelnek, úgy a modern járművek esetében is elengedhetetlen, hogy időben hozzáférjenek a szükséges szoftverfrissítésekhez a gyártóktól. Ezeket a frissítéseket gyakran hagyományos módon, szervizekben végzik el, de egyre népszerűbb az úgynevezett Over-the-Air (OTA) megoldás, melynek keretében az interneten keresztül továbbítják és telepítik a járművekbe a frissítéseket. Ugyanakkor ezt a technológiát a támadók is kihasználhatják, kártékony programok bejuttatásával, amelyek révén hozzáférhetnek a jármű rendszeréhez, személyes adatokat lophatnak, vagy akár az autó fizikai irányítását is átvehetik.

IT BIZTONSÁGI SÉRÜLÉKENYSÉGEK ÉS MEGOLDÁSOK A JÁRMŰIPARBAN

Az informatikai forradalom térhódításával a járműipar is átalakult, amely számos új kihívást és biztonsági problémát hozott magával. Ezen problémák közül jól mutatja a szoftverfrissítés hiányát a Kia incidense, ahol egy hiányzó szoftver modul miatt kialakult a közösségi médiaplatformon zajló úgynevezett "Kia Challenge". Ennek során a "Kia Boyz" néven ismert tolvajok oktatóvideókat tettek közzé arról, hogyan lehet kijátszani a járművek biztonsági rendszerét olyan egyszerű eszközökkel, mint egy USB-kábel. Az incidens számos autólopáshoz, 14 bejelentett súlyos balesethez és nyolc halálesethez vezetett. Ezen kívül biztonsági szakértők 16 autógyártó járműveiben (többek között Ferrari, BMW, Rolls Royce, Porsche) fedeztek fel sérülékenységeket, amelyek lehetővé tették az autó funkcióinak távoli vezérlését ([1]). A sérülékenységek között szerepelt továbbá, hogy a támadók kizárhatják a felhasználókat a távoli járműkezelésből vagy akár megváltoztathatják az autóhoz tartozó felhasználói fiókot, amely mutatja az autókhoz kapcsolódó hitelesítési mechanizmusok fontosságát. Emellett kiemelt a jelentősége annak, hogy az autók műszaki, technológiai paraméterei ma már a korábbinál jóval magasabb szinten állnak, ezáltal a tulajdonsoknak könnyebb elérni az aktuális információkat az autók állapotáról. Azonban számtalan esetben kerülnek ezen adatok meghamisításra, ami komoly bizalmatlanságot teremt például a használt autópiacon. A jelenlegi autóimporthoz használt szabályozások és keretek nem megfelelőek, sokszor hiányosak, amely indokolja erre a problémára egy transzparens és nem hamisítható rendszer kialakítását. A blokklánc tulajdonságai, mint a nyilvános főkönyv, a blokklánc elemeinek módosíthatatlansága vagy az adatok nagyobb rendelkezésre állásának biztosítása jól alkalmazható ezen problémára, amelyet demonstrál többek között az Alfa Romeo gyár, ahol már az egyes modelleknél NFT-ben rögzítik a jármű különböző adatait. A jármű adatainak tokenjéről tanúsítványt állítanak ki, melynek segítségével biztosítható, hogy az autót megfelelően karbantartották. Ez pozitív hatással lehet az autó marad-

ványértékére ([2]). A [3] cikkben egy megbízható, járművek adatait tartalmazó adatbázisrendszert javasoltak a szerzők, amely szintén blokklánc technológiát alkalmaz és az Ethereum platformra épül. A rendszer engedélyköteles láncot használ, melynek segítségével egy megbízható harmadik fél (pl. karbantartó üzem és kormányzati hivatal) rögzítheti a jármű adatokat a blokkláncra, így a járműadatok integritása megőrizhető és ellenőrizhető. A rendszer előnyei közé tartozik, hogy az ügyfelek könnyen lekérdezhetik a releváns járműinformációkat a rendszerfelületen keresztül és elkerülhetik, hogy hamis járműinformációkat kapjanak.

Mivel az autóipar komplex értéklánccal rendelkezik, ezért az információk pontossága és hitelessége alapvető fontosságú. Az autóalkatrészek gyártásától kezdve azok összeszerelésén át egészen a járművek értékesítéséig és karbantartásáig a blokklánc lehetőséget kínál a folyamatok ellenőrzésére és optimalizálására. A gyártók és a beszállítók közötti tranzakciók megkönnyítésétől kezdve a járművek történetének hiteles dokumentálásáig a blokklánc javíthatja az iparág átláthatóságát és csökkentheti a csalások kockázatát. Összegezve a blokklánc technológia alapvető tulajdonságait, mint az adatintegritás biztosítása, a transzparencia, az elosztottság, a decentralizált működés és a kriptográfiai primitívek garantálják az információk manipulálhatatlanságát növelve az ügyfelek és az iparág szereplőinek bizalmát.

BLOKKLÁNCCAL KAPCSOLATOS FOGALMAK

Az általunk javasolt autómobil környezetben alkalmazandó blokklánc alapú rendszer megértéséhez szükséges, hogy a hozzá kapcsolódó fogalmakat meghatározzuk.

Blokklánc

Egy peer-to-peer, elosztott főkönyv (distributed ledger), amelynek a biztonságát kriptográfiai primitívek garantálják, csak bővíthető művelettel rendelkezik (append-only), nem hamisítható és a résztvevők közötti konszenzus vagy megállapodás révén frissíthető. A blokklánc blokkok sorozata, melyeket kriptográfiai hash függvényekkel kötnek össze (hash-lánc), ezáltal a blokklánc teljes története megváltoztathatatlan (immutable). A hash függvény olyan algoritmus, mely egy tetszőleges hosszúságú bemeneti adatot egy fix hosszúságú karakterlánccá képez le. A hash függvény alapvető tulajdonsága az ütközésmentesség, a lavinahatás és az irreverzibilitás. A blokklánc egyes blokkjaiban lévő adatokat tranzakcióknak hívjuk, melyeket elosztottan, több csomópont tárol. A tranzakció egy a felek által digitálisan aláírt műveletek sorozata, amely a blokklánc főkönyvében kerül rögzítésre ([4]). A főkönyv egy adatbázis, amely tartalmazza az összes tranzakciót, amelyet a blokklánc hálózatában végrehajtottak. A decentralizáció az egyik legjelentősebb tulajdonsága a blokkláncnak, ahol nincs szükség megbízható harmadik félre vagy közvetítőre a tranzakciók érvényesítéséhez. A résztvevők a hálózaton keresztül időbélyegezik és ellenőrzik minden egyes tranzakciót. Résztvevőnek tekinthető minden olyan fél, aki tagja a blokkláncnak. ([5][6])

Ethereum

Az Ethereum (ETH) egy nyílt forráskódú, decentralizált blokklánc platform, amely okosszerződést (smart contract) használ. Az Ethereum hálózaton számos számítógép (node) működik és futtatja az Ethereum virtuális gépet (EVM), amely lehetővé teszi az Ethereum

állapotgépének folyamatos, megszakítás nélküli és változatlan működését, valamint az okosszerződések futtatását. A konszenzus mechanizmus biztosítja, hogy az összes csomópont ugyanazon az állapoton dolgozzon, és elfogadja az egyetlen, hiteles változatot az állapotról. Ezáltal lehetséges az egyének közötti konszenzus megvalósítása. Aki részt vesz az Ethereum hálózatban, annak egy másolattal kell rendelkeznie az EVM állapotáról, ezen felül bárki küldhet kérést az EVM részére, hogy tetszőleges számításokat végezzen rajta. Ilyen fajta kérések esetében a hálózat többi résztvevőjének ellenőrizni, validálni és végrehajtani kell a kért számításokat. A számítási kéréseket tranzakciós kéréseknek nevezzük, ahol az összes tranzakció és az EVM állapotának nyilvántartása mind a blokkláncon szerepelnek, amelyet az összes csomópont elosztva tárol és egyeztet. A platform natív kriptovalutája az Ether. A Bitcoin (BTC) után az Ethereum a második legnagyobb és legaktívabban használt kriptovaluta a piacon, egy pont-pont (peer-to-peer) hálózat, ahol a csomópontok konszenzus mechanizmus segítségével működtetik a blokkláncot. Az Ethereumra jellemző a Turing teljesség, ami Alan Turing által meghatározott fogalom. A Turing teljesség magába foglalja, hogy egy adott számítási rendszer vagy modell képes szimulálni bármely más számítási modellt vagy rendszert. Egy számítási modell csak akkor tekinthető Turing teljesnek, ha képes szimulálni minden olyan algoritmust, amely végrehajtható egy Turing-gépen. ([4][5])

Konszenzus mechanizmus

A konszenzusmechanizmus olyan lépések összessége, amelyeket a blokklánc legtöbb vagy összes csomópontja tesz annak érdekében, hogy megállapodjon egy javasolt állapotról vagy értékről. Az Ethereum konszenzus mechanizmust használ, ami 2022 előtt a PoW (Proof-of-Work) volt azonban napjainkban már a PoS (Proof-of-Stake) használatos ([4]). A mechanizmus cserére azért volt szükség, mert a PoS gazdasági szempontból biztonságosabb, hatékonyabb és kevesebb erőforrást igényel, mint a PoW mechanizmus. A konszenzus mechanizmusban azok a résztvevők játszanak kulcsszerepet a hálózat integritásának és biztonságának fenntartásában, akik jelentős mennyiségű Ethereum tokent letétbe helyeznek. Ezzel biztosítják, hogy a hálózaton belüli döntéshozatalban és tranzakciók validálásában a legtöbb tokent birtokló résztvevőknek legyen a legnagyobb befolyásuk, miközben rosszindulatú cselekvés esetén a bizalom megrendülhet és a letétbe helyezett tokenjeik elértéktelenedhetnek. Az Ethereum hálózatán belül a legtöbb tőkével rendelkező résztvevők nagyobb érdekeltséggel rendelkeznek a hálózat biztonsága és fenntarthatósága iránt. Ennek következtében kevésbé valószínű, hogy rosszindulatúan viselkednek, vagy kárt okoznak a hálózatban. Míg a PoW-alapú rendszerekben a támadások jelentős számítási erőforrásokat igényelnek, a PoS mechanizmusoknál a támadások nagyarányú token letétbe helyezését követelik meg, ami különböző kockázatokat és költségeket jelent a támadók számára. Az Ethereum platform fejlesztői eszköztárban található tesztkörnyezet alapvetően a PoW konszenzus mechanizmust alkalmazza. Ugyanakkor az Ethereum Virtual Machine (EVM) strukturális kialakítása kínál egy integrált keretet, melyben az Ethereum Client másnéven Ethereum Validator szerepel. Ez a kliens magában foglal egy Execution Engine-t, amely a tranzakciók megfelelő futtatását garantálja, illetve a Beacon Node-ot, amely a konszenzus mechanizmus koherens végrehajtásért felelős. Az Ethereum platform jellegzetes rugalmasságának köszönhetően a fejlesztők képesek testre szabni a tesztkörnyezetet úgy, hogy többféle konszenzus mechanizmus közül kiválasztják a legoptimálisabbat a projekt igényeinek megfelelően.

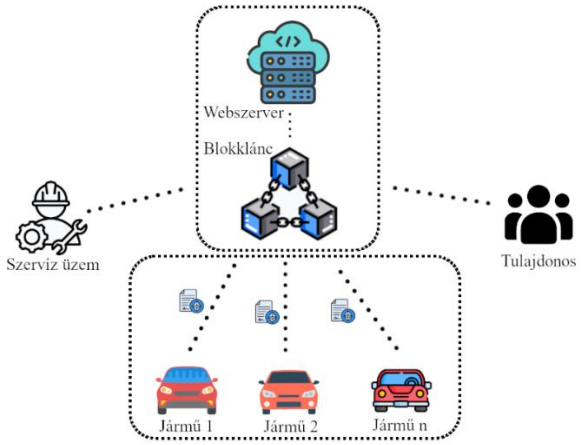
Okosszerződés

Az okosszerződés egy önmagát végrehajtó számítógépes program, amely képes vizsgálni az adott szerződés feltételeinek teljesülését a felek között. Ezek a szerződések sok esetben blokklánc technológián alapulnak, amely egy biztonságos és decentralizált környezetet biztosít a tranzakciók végrehajtásához és tárolásához. Az EVM az Ethereum blokklánc egy olyan alapvető technológiája, amelynek fontos szerepe van okosszerződéseken. Ez a virtuális környezet lehetővé teszi, hogy a blokkláncon tárolt szerződések végrehajthatók legyenek az Ethereum hálózaton. Az EVM pontosabban egy biztonságos futtató környezet, amely garantálja a kódok megbízható végrehajtását, mindeközben kihasználja a blokklánc előnyeit. Széleskörű felhasználási lehetőséget kínálnak, beleértve a pénzügyi tranzakciókat, a beszerzési láncok kezelését vagy a felhasználók profiljához tartozó adatok ellenőrzését. Az okosszerződések elosztott számítógépes programok, amelyek tartalmazzák a szabályokat és a feltételeket. Ha a feltételek teljesülnek a szerződés automatikus végrehajtja az intézkedéseket anélkül, hogy emberi beavatkozásra vagy harmadik felek bevonására lenne szükség. Mivel az okosszerződés blokkláncon működik, így megváltoztathatatlanok és manipulálhatatlanok a kriptográfiai primitíveknek köszönhetően, ezáltal a szerződés feltételei is ugyanezeket a tulajdonságokat örökli. Az EVM-en futtatott okosszerződések gyakran a Solidity programozási nyelvvel készülnek, de léteznek más nyelvek is, mint például a Vyper, Bamboo vagy Serpent, amelyeket szintén használnak Ethereum okosszerződések készítéséhez, ezáltal megvalósulhat az Ethereum blokkláncra való fejlesztés. ([4][7])

JAVASOLT KERETRENDSZER

A járműiparban újonnan megjelenő és a használt autópiacon folyamatosan növekvő számú autómobilokra kidolgoztunk egy olyan keretrendszert, amely képes az adott járműhöz tartozó összes szenzitívnek tekinthető fizikai (kilométeróra állás, alváz szám, hengerűrtartalom, teljesítmény, jelenlegi állapot, előélet) és logikai (szoftver/firmware azonosító, beépített szenzorok által mért adat, biztosítás, diagnosztika által mért adat) attribútumok kezelését, továbbítását és tárolását megvalósítani blokklánc technológia segítségével. Járművek sokasága alkotják az általunk felügyelni kívánt környezetet. Minden autómobilról külön-külön képesek vagyunk az attribútumaikat okosszerződések segítségével kezelni és továbbítani blokkláncra. Ebben az esetben minden jármű egy csomópontnak felel meg és az EVM segítségével képesek vagyunk az okosszerződések kezelésére. A blokkláncot adattárolás szempontjából tartjuk fontosnak emellett teljesíti a megkövetelt bizalmasság (engedélyköteles), integritás és rendelkezésre állás tulajdonságait. A tulajdonos, a szervizműhely, a webszerver és a blokklánc közötti kommunikációhoz TLS (Transport Layer Security) protokollt alkalmazunk. Az adatok és a rendszer integritása érdekében több kriptográfiai primitívet implementálunk, mint például a digitális aláírás és az SHA-256 hash függvény. Az elosztott alkalmazások (DApp) és tárolás nagyobb rendelkezésre állást biztosít emellett a keret kialakítása során figyeltünk a skálázhatóságra (a felhasználó tetszőleges számú autót kezelhet). A letagadhatatlanság szerepet játszik a felhasználók és a tárolt adatok transzparenciája és nyomonkövethetőség érdekében. Az engedélyköteles blokklánc alkalmazása lehetővé teszi az adatokhoz való hozzáférést a jogosult és hitelesített felhasználók számára. Az adatokat titkosítva tároljuk elosztott módon az AES-GCM szimmetrikus blokktitkosítási algoritmus segítségével. Az elosztott tárolásnak a csalások és egyéb kompromitálások

(ransomware támadás) esetében kialakult adatveszteség és az egyszerű visszaállíthatóság érdekében van meghatározó szerepe. Így a tulajdonosok közül csakis azok férhetnek hozzá a tárolt attribútumokhoz, akik rendelkeznek a visszafejtéshez szükséges kulccsal, vagyis csak a jármű tulajdonosa férhet hozzá a saját járműve adataihoz. A webszerver az általunk elkészített járműkezelő felületet valósítja meg egy felhasználóbarát platform keretein belül. A webszerver semmilyen adatot nem tárol, csakis a járműadatokhoz való egyszerű hozzáférhetőséget és módosítások menedzselését teszi lehetővé a tulajdonos és szervizműhelyek számára. Kétfaktoros hitelesítést alkalmazunk, ahol az első faktor esetében a felhasználónak blokklánc fiókkal kell rendelkezni és ez által tagjának kell lennie az adott láncnak (felhasználó név és jelszó páros), majd a második faktor a járműkezelő felülethez való csatlakozást megelőzően egy a felület által generált OTP (One Time Password) megadásával képes hozzáférni a felülethez.



1. Ábra: Blokklánc alapú alkalmazás autómobil környezetre, saját szerkesztés.

ÖSSZEHASONLÍTÁS

A tudományos irodalomban és gyakorlati megvalósításokban több blokklánc alapú megoldást is javasoltak a használtautó piacra. A [8] cikkben bemutatott megoldás az általunk javasolt rendszerhez hasonló célokat valósít meg, ahol kiemelt hangsúlyt kap a használt autók adatintegritása és átláthatósága. Figyelembe veszik az általunk is alkalmazni kívánt eladók és vevők szempontjait egy új vagy használt autó vásárlása esetén. Dél-Koreában a használt autó piac mérete és az autók tranzakciójának száma folyamatosan nő. Ezen a piacon gyakran előfordulnak mulasztások az eladó és a vevő közötti információ aszimmetria miatt. A [8] tanulmányban egy használt autó tranzakciókezelő rendszert javasolnak, amely a nyilvános blokklánc Ethereumon alapuló okosszerződések segítségével garantálja a megbízhatóságot harmadik felek beavatkozása nélkül. A nyilvános blokkláncot a használt autó tranzakciókezelő rendszerben alkalmazták az autók információjának megbízhatósága alapján egy biztonságos és megbízható tranzakciókezelő rendszer tervezésére. Az okosszerződéseket a használt autó kereskedési szerződések tervezésére (adásvételi szerződés) és adat továbbításra használták. A rendszer csökkenti az információ aszimmetriát a vevők és az eladók között a blokklánc integritása és átláthatósága révén. Az adattároláshoz az IPFS-t

(InterPlanetary File System) használták, ahol hash értékeket adtak vissza az okosszerződésekben, amelyeket egy Mongo adatbázison alapuló Node.js szerverben tároltak. Amikor egy új autó eladására kerül sor, a tulajdonos egy böngészőn keresztül fér hozzá a platformhoz, ahova képes manuálisan feltölteni a járműhöz tartozó adatokat. Ezek az adatok átmenetileg a Mongo adatbázisban kerülnek tárolásra, majd okosszerződések segítségével lesznek véglegesítve a blokkláncon. A Korea Fogyasztói Ügynökség szerint a használt autók károk miatti kárelhárítási kérelmek száma csökken, de a használt autók teljesítményének és állapotának ellenőrzési aránya növekszik. A használt autó tranzakciók okozta károk 80%-a hamis információk miatt keletkezik. A használt autó kereskedelmi rendszer átfogó sémája hét entitásból áll: vásárló, bankokkal társított partnercég, használt autó, javítással kapcsolatos partnercég, használt autóértékesítési cégek, munkaadók és munkaadókat kezelő entitás.

A [9] cikkben az általunk alkalmazni kívánt technológiákat és védekezési mechanizmusokat gyűjtötték össze. A járműpiac az emberi civilizáció egyik legnagyobb gazdasági ágazata. Ez egy létfontosságú és folyamatosan változó piac, amelynek közvetlen hatása van az emberi életre, a biztosítási társaságokra, a kormány költségvetésére, a nyereségre és a költségekre. Problémát jelentenek a kilométer óraállás manipulációja a javítóműhelyek és az autókereskedések által, mivel a járműtörténeti nyilvántartások papíralapúak így elveszhetnek vagy károsodhatnak. Továbbá ezek a nyilvántartások megváltoztathatóak és manipulálhatóak, amely komoly aggodalomra ad okot és évente körülbelül 5,6 és 9,6 milliárd eurós kárt okoz az európai fogyasztóknak. A használt járműpiac csalásmegelőzésére számos javaslatot tettek, mint például a használt járművek valóságos árainak automatizálása statisztikai adatok alapján és gépi tanulási technikák alkalmazásával (k-legközelebbi szomszéd algoritmus, naiv Bayes osztályozó), illetve sokan az óraállás csalások megelőzésére összpontosítottak statisztikai adatokat figyelembe véve. Az eddigiekben tárgyalt megoldások többsége statikus jármű adatok kezelést elemeztek, azonban nem vették figyelembe a dinamikus jármű adatok kezelését, továbbítását és tárolását, illetve hogyan lehet ellenőrizni az adatok érvényességét és hitelességét. 2017-ben a Renault csoport és a Microsoft csapat közreműködésük során megalkották az első digitális autókarbantartási könyv prototípusát ([10]). 2019-ben VINChain projekt ([11]) egy blokklánc alapú megoldást javasolt a járművekre vonatkozó adatok elosztott tárolására. 2019-ben a Car-Vertical projekt esetében az autóhoz tartozó állapot adatokat tárolták, mint például kilométer óraállás, márka, totálkár azonban az autó szervízelésével kapcsolatban nem tároltak adatokat. 2017-ben Chanson egy rendszert javasolt a kilométer óraállás manipuláció megelőzésére, ahol a blokkláncot, mint adatvédelmi eszközt használja ([12]). A rendszer rögzíti az autó kilométeróráját és GPS adatait egy dongle (hardverkulcs) segítségével és rögzíti azokat az Ethereum blokkláncra. Egy alkalmazás az eszközön belül fogadja az adatokat Bluetooth segítségével, majd elküldi az adatok hash értékét. Az adatokat a felhasználó privát kulcsával írják alá az Ethereum blokkláncon. Az alkalmazás titkosítja az adatkészletet és elküldi egy privát, biztonságos felhő adatbázisba.

Míg az [8] és [9] tanulmányok különböző technológiákat és megközelítéseket alkalmaznak, és néhány adatot vagy nem tárolnak, vagy csak bizonyos esetekben, saját rendszerünk egy átfogó, integrált megoldást kínál a járművek összes releváns adatának tárolására, az elosztott tárolási és alkalmazási lehetőségekkel kombinálva. Ezzel nem csak a járműpiac adatintegritásának és átláthatóságának növelését célozzuk meg, hanem a rendszer teljes körű biztonságát és megbízhatóságát is. A [8] megoldásban előnyként emelhető ki a

tárgyalt keretrendszer tesztkörnyezetben alkalmazott megvalósítása, hiszen valós környezetben láthatóak a rendszer erősségei és esetleges hiányosságai, így növelhető a felhasználói élmény a visszajelzések alapján. Ezentúl a rendszer csökkenti a vevők és az eladók közötti információ aszimmetriát. Azonban a publikus blokklánc alkalmazása jogosulatlan felek közbeavatkozását teszi lehetővé, ami befolyásoló tényező lehet az adatok integritásának megőrzése érdekében. Emellett az okosszerződések sokkal több funkciót látnak el, ami a fejlesztők számára nehézségeket jelenthet esetleges problémák megelőzése vagy helyreállítása esetén. A [9] cikkben több alkalmazott technológiáról olvashatunk, amelyek mindegyike külön-külön egy jól működő, adott területet lefedő alkalmazás. Hátrányként emelhető ki, hogy a technológiákról együttesen nem készült egy összefogó implementáció, ami egy jól kidolgozott keretrendszerhez vezet. Az általunk javasolt keretrendszer előnyei közé tartozik a kidolgozott és már alkalmazható implementáció, ami blokklánc alkalmazásával a biztonságos identitás- és hozzáférés- kezelést, illetve az elosztott tárolást, alkalmazást és az adatok tárolását, kezelését valósítja meg. Azonban további kutatási célként megfogalmazva, a hátrányok közé soroltuk a saját rendszerünkben a kulcsmegosztással kapcsolatos felmerülő hatékonyabb protokoll létezését a szervizműhelyek és az autótulajdonosok között. Az 1-es táblázatban az általunk javasolt rendszer előnyeit és hátrányait vetettük össze a [8] és [9] tanulmányban felsorolt megoldásokkal.

A feldolgozott megoldások mindegyikénél fontos szempont volt az információ aszimmetria csökkentése és a transzparencia növelése és a felhasználó barát alkalmazás megvalósítása. Azonban eltérések mutatkoznak a rendszerek között, mint például a járművekhez tartozó adatok feldolgozási módja, a blokklánc technológia és alkotó elemeinek alkalmazási módja és a biztonsági követelmények teljesülése.

Tanulmányok	Előnyök	Hátrányok
Seung Gyun Yoo, Byeongtae Ahn [8]	• Tesztkörnyezetben alkalmazott rendszer Dél-Korea térségében • Információ aszimmetria csökkentése • Transzparencia.	• Publikus blokklánc • Okosszerződések nem megfelelő alkalmazása
Sara El-Swtiti, Mohammad Qatawneh [9]	• Alkalmazott technológiák részletes elemzése	• Nincs összefogó kidolgozott implementáció
Általunk javasolt megoldás	• Kidolgozott és alkalmazható rendszer • Engedélyköteles blokklánc • Elosztott adattárolás és alkalmazás	• Nincs hatékony kulcsmegosztás a szervizműhelyek és a felhasználó között • Még nem alkalmazott tesztkörnyezeten kívül

1. Táblázat: Alkalmazott rendszer összehasonlítása, saját szerkesztés.

ÖSSZEFOGLALÁS

A cikkben feltérképezésre kerültek az autóipar digitalizációjának nehézségei és egy transzparens engedélyköteles blokklánc alapú rendszert javasoltunk ezen problémák kezelésére. Figyelembe vettük a tudományos és gyakorlati blokklánc alapú megoldásokat a használt autó piacon. Emellett kifejtésre kerültek a szükséges fogalmak és kapcsolódó technológiák, amely egy általunk javasolt keretrendszer alkalmazásához szükségesek. Végezetül összehasonlítást végeztünk a rendszerünk és a több tudományos irodalomban javasolt megoldás között, ahol kiemeltük a kapcsolódó előnyöket és a hátrányokat egyaránt. Célunk a kiber-ellenálló képesség növelése, a transzparencia és a csalások csökkentése a használtautó-piacon. A későbbi kutatási cél, hogy továbbfejlesszük a javasolt rendszert és kibővítsük egy hatékonyabb kulcsmegosztással a szervizműhely és az autótulajdonos között.

FELHASZNÁLT IRODALOM

[1] Curry S., “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More” in *Samcurry.net*, 2023. [Online] Elérhető: https://samcurry.net/web-hackers-vs-the-auto-industry/

[2] Vitelaru E., & Persia L., *Fractional Vehicle Ownership and Revenue Generation Through Blockchain Asset Tokenization.* Transport and Telecommunication Journal, 24(2), 120-127, 2023.

[3] Jiang, Y. T., & Sun, H. M., *A blockchain-based vehicle condition recording system for second-hand vehicle market.* Wireless Communications and Mobile Computing, 1-10, 2021. [Online] Elérhető: https://doi.org/10.1155/2021/6623251

[4] Ethereum, 2023. [Online] Elérhető: https://ethereum.org/en/developers/docs/intro-to-ethereum/

[5] Bashir I., *Mastering Blockchain*. Packt Publishing Ltd. Birmingham, 2020.

[6] Md Ashraf Uddin, *Introduction to Blockchain Technology*. Federation University Australia, Jagannath University, pp. 1-2, 4, 14-20, 2021. [Online] Elérhető: https://www.researchgate.net/publication/356784725

[7] Zheng G., Gao L., Huang L. & Guan J., *Ethereum Smart Contract Development in Solidity*, 2021. [Online] Elérhető: https://books.google.hu/books?id=OGn6DwAAQBAJ&lpg=PR7&ots=_g2xRs3S7I&dq=smartcontract%20and%20solidity&lr&hl=hu&pg=PA3#v=onepage&q&f=false

[8] Yoo G. S.& Ahn B., *A study for efficiency improvement of used car trading based on a public blockchain.* The Journal of Supercomputing, 2021. [Online] Elérhető: https://doi.org/10.1007/s11227-021-03681-z

[9] El-Switi S. & Qatawneh M., *Application of Blockchain Technology in Used Vehicle Market: A Review*. International Conference on Information Technology (ICIT), 2021. [Online] Elérhető: https://www.researchgate.net/publication/353488375

[10] Automotive World, *Groupe renault teams with Microsoft and Viseo to create the first-ever digital car maintenance book prototype*. 2017. [Online] Elérhető: https://www.automotiveworld.com/news-releases/groupe-renault-teams-microsoft-viseo-create-first-ever-digital-car-maintenance-book-prototype/

[11] Vinchain, *Decentralized Vehicle History — Car Accident History Check by VIN*. 2019. [Online] Elérhető: https://vinchain.io

[12] Chanson M., Fleisch E., Bogner A. & Wortmann F., *Blockchain as a privacy enabler: an odometer fraud prevention system*. ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers. 2017. [Online] Elérhető: https://www.researchgate.net/publication/319602303

PÁLYÁZATRA UTALÓ MEGJEGYZÉS

A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM ÚNKP-23-1 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.