Hyperledger Fabric hálózat létrehozása az energiamenedzsment adatainak biztonságos tárolása érdekében

Bálint Krisztián

balint.krisztian1@uni-obuda.hu

Absztrakt A megújuló energiaforrások felhasználásával a környezetünkre gyakorolt káros hatások csökkenthetők. Ez a technológia azonban még mindig hatalmas fejlődés alatt áll, hiszen évről évre jelennek meg új megújuló energia megoldások, amelyek hatékonysága folyamatosan növekszik. A kutatási célja, hogy részletesen megvizsgálja a Hyperledger Fabric struktúra lehetőségét érzékeny energiagazdálkodási adatok blokkláncban való tárolására mindezt annak érdekében, hogy illetéktelenek ne csatlakozhassanak a különböző mikrogridhez. Fontos szempont, hogy illetéktelenek ne hozzáférjenek hozzá a peer entitások adataihoz, azok ne kompromitálódjanak. A gyakorlati megvalósítás részeként egy Hyperledger Fabric jogosultságú hálózat kerül létrehozásra, amely blokklánc technológián alapuló felépítésénél fogva biztonságosan tudja kezelni az érzékeny energiamenedzsment rendszer adatait. Az empirikus kutatás részeként a szerbiai és magyarországi egyetemisták nézőpontját kerül feltárásra a Hyperledger Fabric hálózaton keresztül tárolt energiagazdálkodási rendszerről. A felmérésre azért van szükség, mert a jövőben feltételezhető, hogy a jelenlegi hallgatói generáció lesz az ehhez hasonló rendszerek felhasználója és széles körben el fog terjedni a felhasználók között. A kutatásból kiderült, hogy a biztonságos adattárolás és a megújuló energiagazdálkodási rendszer valóban fontos mindkét ország egyetemistái számára, hiszen ezek az előremutató megoldások szükségszerűek lehetnek a nem túl távoli jövőben.

Kulcsszavak: Hyperledger Fabric, blokklánc technológia, energiamenedzsment alapú rendszer, megújuló energia.

Bevezető

A megújuló energiaforrások felhasználása szükségszerű, hiszen az ipari és elektronikai fejlődésnek köszönhetően megsokszorozódott a villamosenergia-igény, amelyet megújuló energiaforrásokkal célszerű helyettesíteni a környezet és a bolygó védelme érdekében. Ezek az új megújuló energia trendek hatalmas jelentőséggel bírnak, ez által alapjaiban változtatják meg a Világ legtöbb országának fejlődési trendjeit [1]. A környezet védelme megújuló energiaforrások

használata nélkül fenntarthatatlan állapot és mindenki számára egy veszélyes jövőkép.

A decentralizált blokklánc technológiának köszönhetően az energiagazdálkodási szektor fejlesztése hatékonyan megvalósítható, hiszen ezek a megoldások felgyorsíthatják az energiahálózatok szabályozását, ugyanakkor növelhetik az adatbiztonságot is. E két kulcstényező megléte nagyban támogathatja a megújuló energiagazdálkodást. Megfigyelhető, hogy a P2P (Peer-2-Peer) hálózati struktúrának köszönhetően a megújuló energia értékesítése biztonságosan megvalósítható az energiatőzsdén, valamint számos ipari területet érintő kvóták számára is biztonságos adattárlást tesz lehetővé. A mikrohálózatok a jövőben még inkább elterjednek, hiszen jelenleg is növekvő tendenciát mutat a lakosság energiahálózatba történő megújuló energiaellátása táplálása.

A blokklánc technológia használatával időt és pénzt lehet megtakarítani, hiszen nincs szükség harmadik félre, valamint az adatokhoz jogosultságtól függően könnyen és biztonságosan is hozzá lehet férni. Napjainkban a központosított adattárolás kevésbé biztonságos, mivel az érzékeny adatokat központilag tárolják, amely számos veszélyt jelenthet az érzékeny adatok számára [2].

A hatékony adatvédelem nem állandó állapot. A mai rohanó világban be kell látnunk, hogy a bizonytalanság állandó, és váratlan helyzetekben szembe kell néznünk vele [3]. A 21. század eleje óta a Világ számos súlyos számítógépes bűnözővel szembesül, amely azt mutatja, hogy az emberek egyre inkább függnek a technológiai fejlődés hasznosságától [4].

Az informatikában hatalmas fejlődés zajlik az energiamenedzsment alapú rendszerek ezen területen, valamint új funkciók jelennek meg, amelyek a hatékonyságot hivatottak növelni. Ahhoz, hogy ez a megoldás széles körben elfogadottá váljon, olyan új megoldásokat kell kialakítani, mint például a biztonságos adattárolás, így elkerülhetők a jövőbeni incidensek.

A Hyperledger Fabric blokklánc technológiát alkalmazó biztonsági megoldások hatékonyan tudják tárolni az energiamenedzsmenti rendszer érzékeny adatait és azokat elérhetővé válnak a csomópontban az arra jogosult személyek számára. A kutatás a következő struktúra szerint épül fel:

- Energiagazdálkodási megoldások vizsgálata a Hyperledger Fabric hálózat létrehozása előtt, a még hatékonyabb és biztonságosabb adattárolás érdekében,
- Blokklánc alapú Hyperledger Fabric hálózat létrehozása.
- Az empirikus kutatás részeként magyarországi és szerbiai hallgatók lettek megkérdezve arról, hogy szerintük a Hyperledger megoldást alkalmazó hálózati blokklánc a véleményük szerint alkalmas-e az adatok biztonságos tárolására.

Energiagazdálkodási megoldások alkalmazása blokklánc technológia alkalmazása által

A blokklánc technológia alkalmazásával energiamenedzsmenti megoldások hozhatók létre a blokkláncban. Ez azt jelenti, hogy a csomópontok biztosítják az adatok biztonságos tárolását. A rendszer megvalósításánál fontos ügyelni arra, hogy az adatok a csomópontokban arányosan, darabokra bontva kerüljenek mentésre. Így ha egy célzott támadás érné a csomópontot, még a legrosszabb esetben is csak egy kis adat kerülne illetéktelenek birtokába. Ennek ellennére célszerű az adatokat titkosítani még azok feldarabolása és feltöltése előtt, így lehetetlenné téve az adatok értelmezését illetéktelen személyek számára. Ahhoz, hogy illetéktelen személy hozzáférjen minden egyes energiagazdálkodási célból tárolt adathoz, a teljes blokkláncot fel kell törnie, amely a decentralizáltságából kifolyólag szinte kivitelezhetetlen feladat, mivel nem áll mögötte központi kiszolgáló szerver.

A mikrohálózatok a modern energiaiparra jellemző tulajdonságokkal rendelkeznek, mint például az adatok több egységes régióra és eszközre való osztása. Fennáll azonban a kulcs elvesztésének és kulcsszivárgásának a kockázata, továbbá az összetett feldolgozási folyamatokban a hitelesítési entitások közötti tanúsítványok is kompromitálódhatnak. Komolyabb informatikai beavatkozást igényelne az intelligens terminálok biztonságának növelése a megbízható adathozzáférés megvalósítása érdekében. Az engedély nélküli blokkláncok lehetővé teszik az elosztott konszenzust anélkül, hogy előzetesen létező identitást vagy megbízható harmadik felet hoznának létre [5].

A decentralizált energiarendszer hatékonyabb menedzselése érdekében a jövőben ajánlatos lenne a blokkláncot használni a hatalmas mennyiségű adatok tárolására, a fogyasztók adatainak védelmére, illetve a konszenzusos döntéshozatalra. A blokklánc technológiák egyszerűbbé és igazságosabbá teszik a decentralizált energiarendszerek használatát, valamint csökkentik a kezelési költségeket. A rendszerre jellemző, hogy leginkább akkor a leghatékonyabb, ha a résztvevők száma nő, amelyel a decentralizált irányítási mechanizmus könnyedén megbirkózik [6].

A főkönyvi hálózat elosztott főkönyvi csomópontokból áll. Minden elosztott főkönyvi csomópont ugyanazt a főkönyvi információt tárolja szinkronizálva, ez által biztosítva a tisztességes tranzakciót, így fenntartva a rendszer stabilitását. Általában amikor egy elosztott főkönyvi csomópont energiaadatokat tölt fel egy adathalmazból és intelligens rendszerekből, akkor először lefuttatja a konszenzusos mechanizmust, majd átadja a rendszer biztonsági ellenőrzését, abból kifolyólag hogy biztosítsa az adatok pártatlanságát és a rendszer biztonságát.

Az elosztott főkönyvi csomópont ellenőrzése után a felhasználó szabadon részt vehet a csomóponti hálózatban, vagy kiléphet onnan, ami azt jelenti, hogy ennek a hálózatnak van egy skálázhatósága a feltöltési sebesség és megbízhatóság fenntartása érdekében [7].

Hyperledger Fabric hálózati megoldások

A Hyperledger Fabric (az egyszerűség kedvéért Fabric) által tárolt érzékeny energiagazdálkodási adatok biztonságos tárolása érdekében meg kell vizsgálni a biztonsági architektúra által kialakított megoldásokat, elkerülve ezzel az adatok jövőbeni kompromittálását. A Fabric számos speciális biztonsági funkcióval rendelkezik, amelyek a következő fontosabb megoldásokat használják a konszenzus mechanizmuson keresztül. Ezek a következők:

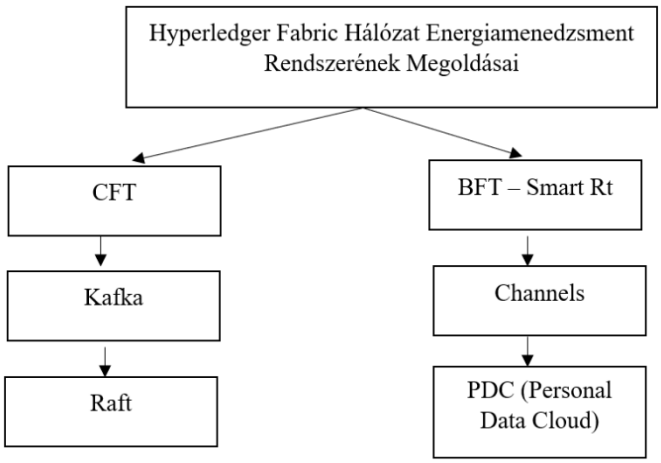
- Kafka - Alkalmazása lehetővé teszi, hogy a rendszer továbbra is működjön, ha hiba történik, és ennek eredményeként bizonyos specifikus tulajdonságokkal rendelkezik [8]. Emellett a hitelesítési mechanizmusa is nagyon hatékony, hiszen ismeri az SSL/TSL, SASL és Kerberos mechanizmusokat is.
- Raft – A konszenzus algoritmus része. A csomópontok fontosak, mivel a vezető sorrend létrehozhat egy új blokkot [9]. Működési felépítése a decentralizált DeFi platformokra jellemző. Egy naplóbejegyzést használ az egyes műveletek rögzítésére, amelyhez a Raft felhasználók hozzáférhetnek és minden bejegyzéshez hozzájárulhatnak.
- CFT (Crash Fault Tolerance). Nagyon fontos, hogy a számítógépek időben kommunikálni tudjanak, amelynek kulcstényezője a megfelelő szinkronizálás. A konszenzus alapú állapotgép replikációnak (SMR) köszönhetően a rendszer meghibásodás esetén is működik [10]. Proof-of-Authority algoritmust használ, amely azt jelenti, hogy hiteles érvényesítőkre van szükség az adatok validálásához és rögzítéséhez. Ez a gyakorlatban azt jelenti, hogy (50% + 1 szavazat) elegendő a közösségi döntés elfogadásához.
- BFT-SmaRt (bizánci hibatűrő – SmaRt). Java alapú megoldás. A rendszer úgymondván “a hibás és nem hibás” ügyfelek működésén alapul. [11]. A BFT-algoritmusok általában 3f + 1 szervert (vagy replikát) igényelnek, hogy elviseljenek egy f bizánci (vagy hibás) szervert. A BFT működésének lényege, hogy a csomóponti hibák mielőbb üzemképesek legyenek, és a helyreállításuk hatékonyan menjen végbe. Azon az elgondoláson alapulnak, hogy a helyes replikák egy szavazatsorozatban legyőzhetik a hibás replikákat, és ehhez legalább f + 1 helyes replikára van szükségük,

összesen 2f + 1 szerveren. Ezek az algoritmusok azonban ennél a minimumnál f több szervert igényelnek [12].

A hatékony adatvédelem érdekében a Fabric a következő megoldásokat használja:

- Csatornák – Lehetővé teszi a biztonságos és titkos kommunikációt a csatornák között. Első lépésben azonosítani kell a csatornához csatlakozó feleket, és csak ezután következhet a titkos kommunikáció. Új csatorna létrehozásához az ügyfél SDK meghívja szükséges amely olyan tulajdonságokra hivatkozik, mint a rendszer tagjai és szervezetei. Az új kérelem egy új blokkot hoz létre, amely konfigurációs információkat tartalmaz a csatornaszabályokról és a tagokról [13].
- A PDC-k (Personal Data Cloud) megoldásait az adatok holisztikus betöltése jellemzi. Az adatokat egy központosított felhőben tárolják, ahol az illetéktelen hozzáférések száma korlátozott [14]. Hátránya, hogy hiányzik a rendszerben az egységes szabályozás, ezért az adatok átadása sok esetben problémát okoz. Továbbá célszerű lenne az adatvédelmi szabályokat is átgondolni, ennek ellenére a PDC nagyobb biztonságot nyújt, mint a nem személyes adatfelhő funkcióival rendelkező megoldások.
- ZKP-k (Zero-Knowledge Proofs). Magas szintű és rendkívül hatékony bizonyítási módszer, amelyben a felek nem ismerik egymást. A személyazonosság igazolása során nem az érzékeny információ biztonságosan tárolható. Az azonosítás során a Zero-Knowledge Proof of Identity (ZKPI) módszert kerül alkalmazásra [15]. A ZKP-k elrejtik az UTXO gráfot [16]. A úgynevezett “zero knowledge - nulla tudás” alatt, mivel a felek nem fedik fel kilétüket, matematikai műveleteket kell megoldaniuk és igazolniuk magukat. A ZKP alapú hitelesítés ezen a módszeren alapul.

A következő 1. ábra a Fabric architektúra felépítését mutatja be biztonságtechnikai szempontok figyelembe vétele mellett.



Ábra 1 Hyperledger Fabric hálózat energiamenedzsment rendszerének megoldásai

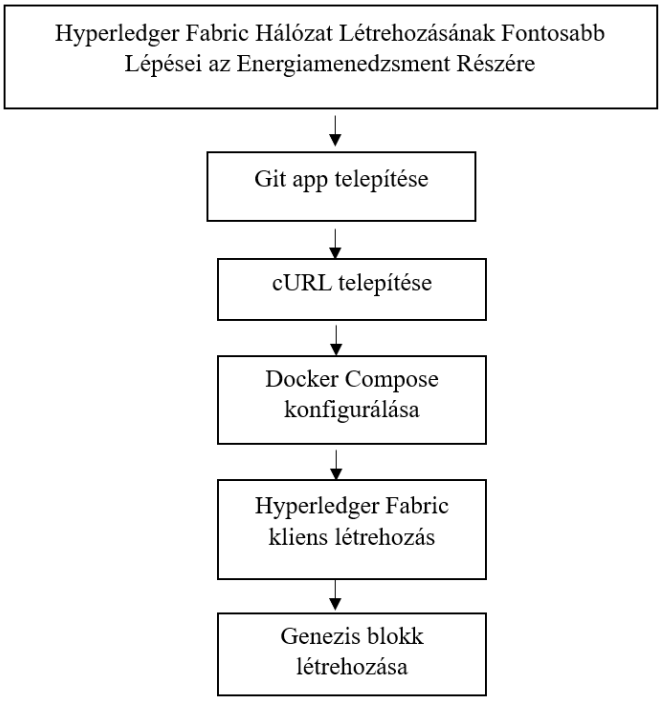
A Fabric megoldásainak áttekintése után megállapítható, hogy az érzékeny és energiagazdálkodási szempontból fontos adatokat biztonságosan képes tárolni, ezért lehetséges, hogy a Fabric az energiamenedzsment rendszer részét képezze.

Hyperledger Fabric hálózat létrehozása

A felhőalapú adattárolás nagy adatterületet biztosít alacsony költséggel. Ez mellett fontos megemlíteni a platformok közötti hatékony átruházhatósági képességet is [17]. Ez minden bizonnyal hatalmas előnye a felhő alapú adattárolásnak.

A hibrid felhő alapú megoldás ötvözi a nyilvános felhő megoldásokat a privát megoldással, ezzel is növelve az adattárolás biztonságát, hiszen sok cég a felhőben tárolja érzékeny adatait [18]. Mivel a blokklánc alapú adattárolás decentralizált, így nincsen szükség hibrid biztonsági megoldásokra.

A Hyperledger Fabric hálózat, amelyt blokklánctehnológiát alkalmaz a létrehozása energiagazdálkodás céljából a következő fontosabb lépésekből áll, amelyet a második ábra mutat be.



Ábra 2 Hyperledger Fabric hálózat létrehozásának fontosabb lépései

A Fabric telepítésének első fontos lépése a Git, a forráskód kezeléséhez használt DevOps eszköz telepítése. Linux Ubuntu operációs környezetben ez a következő paranccsal tehető meg, amely a harmadik ábrán látható.

```
# apt-get install git
# add-apt-repository ppa:git-core/ppa # apt update; apt install git
```

Ábra 3 Git telepítése

Következő lépésként le kell tölteni és telepíteni kell a cURL-t. A gyakorlati megvalósítás során a legújabb cURL 8.8.0 verziót érdemes választani, mivel ez a verzió számos hibajavítást tartalmaz. A cURL-re azért van szükség, mert hasznos a végpontok tesztelésében és a naplózási folyamatban is. A cURL-t az alábbi paranccsal érhetjük el, amely a negyedik ábrán látható.

```
curl -O https://hyperledger.github.io/composer/latest/prereqs-ubuntu.sh
```

Ábra 4 cURL telepítése

A Docker Compose támogatja az adatmegmaradáshoz szükséges köteteket és a szolgáltatások közötti kapcsolati hálózatokat. A Docker Compose hatékony hozzáférést biztosít számos Docker-szolgáltatáshoz. Az ilyen típusú szolgáltatások

számos parancssori felületen (CLI) használhatók [19]. A Docker konfigurációja az alábbi ötödik ábrán látható.

```
Docker Compose version v2.17.3
 docker --version
Docker version 23.0.5
services:
  nginx-service:
    container_name: energy_management
    image: nginx: new
    cpus: 2.0
    mem_limit: 1024m
    ports:80
docker run -d \
  --network todo-app --network- mysql \
```

Ábra 5 Docker konfigurálása

A Fabric Client kapcsolat létrehozásához végpontra van szükség, amely a get-member paranccsal érhető el. Ez az alábbi hatodik ábra prezentálja.

```
fabric_blockchain get-member \
--fabric_n_identification_n-GHDOEL328592KFM233719D3D3F \
--member-identification_m-LGKIXSPT74GKFD834I853FG3LSN
```

Ábra 6 Hálózat és az első felhasználó azonosítása

A csatornakonfiguráció első lépése a Genesis blokk azonosításával kezdődik. Ez az alábbi hetedik ábrán látható.

```
configtxgen -profile SampleAppGenesisRaft -output_first_block genesis.pb -
channel_identification_energy management
```

Ábra 7 Csatornakonfiguráció a Genesis blokkban

Empirikus kutatás

A kutatás fontos aspektusaként jelenik meg a hallgatók blokklánc-alapú alkalmazások felmérésének az igénye. Napjainkban is a Bitcoin megjelenése óta a blokklánc technológia még gyerekcipőben jár, hiszen sok esetben egy decentralizált környezetben működő megoldásokról van szó, amelynek szabályozása nem minden esetben egyértelmű és nem hiányosan definiált. Ennek ellenére célszerű foglalkozni kell vele, hiszen valós és hatékony alternatív megoldást jelenthet a felhőalapú

adattárolásra szempontjából. A környezetvédelem is felértékelődött az elmúlt években, gondoljunk csak az elektromos autók terjedésére.

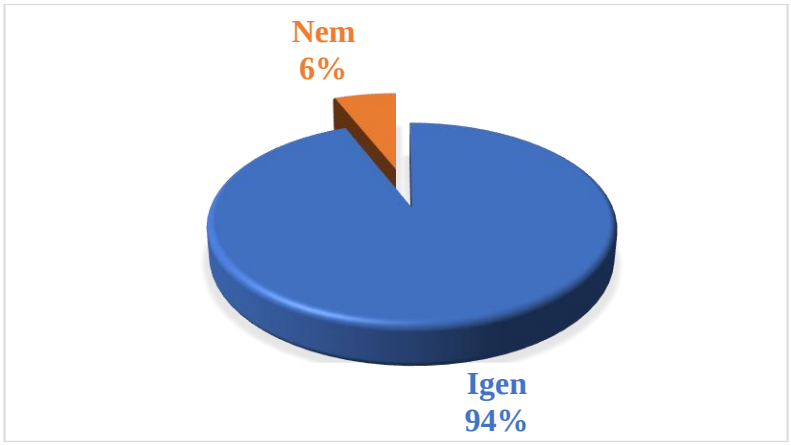
Már csak ezért is fontos betekintést nyerni az egyetemi hallgatók jelenlegi generációjába, mivel feltételezhetően a jövőben ők fogják majd a legtöbbet használni ezeket az új megoldásokat. Az empirikus kutatásban magyarországi és szerbiai egyetemisták vettek részt, ahogyan azt az alábbi első táblázat is részletezi. A hallgatók egy online kérdőívet töltöttek ki és az abban megfogalmazott kérdésekre válaszoltak, amely zárt kérdéseket tartalmazott. A kapott válaszok az SPSS program segítségével lett kielemezve.

Táblázat 1 Hallgatók eloszlása egyetemenként

Országok	**Egyetemek**	**Hallgatók eloszlása egyetemenként**
Magyarország	Óbudai Egyetem, Budapest – Trefort Ágoston Mérnökpedagógiai Központ	28
	Óbudai Egyetem, Budapest – Keleti Károly Gazdasági Kar, Üzleti Tudományok és Digitális Ismeretek Intézet	37
Sezrbia	Singidunum Egyetem Belgrád – Információs Technológiák Intézet	52
	Singidunum Egyetem Belgrád – Elektrotechnikai és számítástechnikai Intézet	49
Hallgatók létszáma		**166**

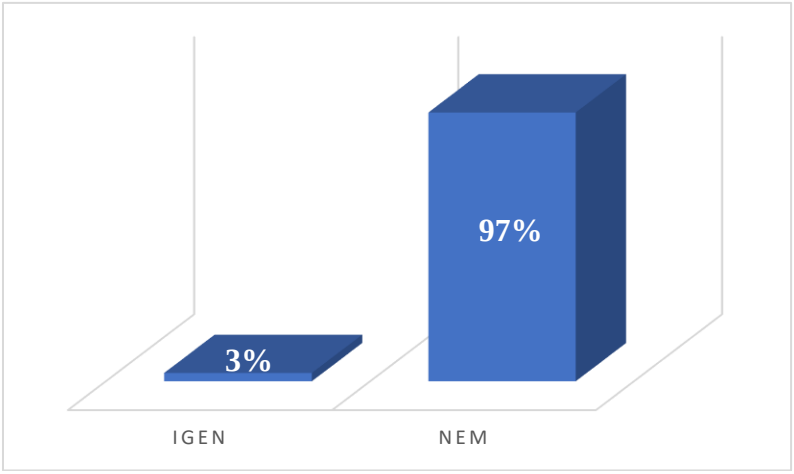
Hipotézis: Feltételezhető, hogy a kutatásba részt vevő hallgatók fontosnak tartják a Hyperledger Fabric Network Blockchain alapú energiagazdálkodási biztonsági rendszer megoldását.

Az empirikus kutatás első kérdése azt kívánja feltárni, hogy a két ország egyetemi hallgatói hogyan vélekednek az energiagazdálkodás részét képező biztonságos adattárolásról. Az egyetemtől függetlenül a hallgatók többsége (khi-négyzet próba: p=0,058) az eergiagazdálkodás szempontjából fontosnak tartják a biztonságos adattárolást. A kapott válaszok eloszlását az alábbi 8. ábra prezentálja.



Ábra 8 Szerinted fontos a biztonságos adattárolás az energiamenedzsmentben?

A Hyperledger Fabric hálózat alapú blokklánc kevésbé elterjedt az informatikában. Ez egy új megoldás, amellyel még az informatikusok is még csak most ismerkednek. A legtöbb hallgató egyetemtől függetlenül (khi-négyzet próba: p=0,053) nemmel válaszolt arra a kérdésre, hogy ismeri-e a Hyperledger Fabric hálózatának felépítését és annak működését. Ez az alábbi kilencedik ábrán látható.



Ábra 9 Ismered a Hyperledger Fabric hálózati megoldást?

Összefoglalás

A megújuló energia felhasználása egyre elterjedtebb, és ez a technológia évről évre folyamatosan fejlődik. Vélhetően a jövőben még inkább elérhetővé válik az emberek számára a megújuló energia felhasználásának lehetősége, így a felmerülő nehézségekre megoldást kell találni. Problémát jelenthet az érzékeny energiagazdálkodási adatok biztonságos tárolása.

A blokklánc technológia minden bizonnyal még gyerekcipőben jár, bár az élet számos területén már bizonyította létjogosultságát. A blokklánc elosztott és decentralizált felépítése miatt az adatok részekre bonthatóak és a csomópontok segítségével biztonságosan tárolhatóak benne az adatok.

A Hyperledger Fabric olyan biztonsági architektúra megoldással rendelkezik, amely az energiamenedzsmentet megfelelő platformmal látja el, így a felhasználók az energiával kapcsolatos adatokat biztonságosan képesek tárolni. Ebben fontos szerepe van a ZKP azonosítási megoldásának is, amelyben a felhasználók kiléte nem sérül.

Jelenleg a Hyperledger Fabric megoldás kevésbé elterjedt, amit az empirikus kutatás is alátámaszt, hiszen a hallgatók még nem hallottak erről a megoldásról. A Fabric segítségével azonban hatékony megoldást képes nyújtani az érzékeny adatok biztonságos tárolása érdekében.

Összegezve megállapítható, hogy a blokklánc technológia a jövőben fontos szerepet tölthet be az energiagazdálkodás területén, hiszen olyan biztonsági megoldásokra épül, amelyeket a központosított felhő alapú rendszerek már nem képesek biztosítani.

Források

[1.] M. Garai-Fodor, “Analysis of Financially Aware Consumer Segments from the Perspective of Conscious Consumer Behaviour“. Acta Polytechnica Hungarica, 20(3), 83-100, 2023.

[2.] J. Lin, M. Pipattanasomporn, S. Rahman, “Comparative analysis of blockchain-based smart contracts for solar electricity exchanges,” In 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5). IEEE. 2019.

[3.] Á. Csiszárik-Kocsir, “The Purposes and Motivations of Savings Accumulation based on Generational Affiliation Financial Education and Financial Literacy“. Acta Polytechnica Hungarica, 20(3), 195-210, 2023.

[4.] T. Nguen Bao Ngo and A. Tick, “Cyber-security risks assessment by external auditors“. Interdisciplinary Description of Complex Systems 19:3 p. 16, pp. pp. 375-390, 2021.

[5.] L. Wang, S. Jiao, Y. Xie, S. Mubaarak, D. Zhang, J. Liu, and M. Li, “A permissioned blockchain-based energy management system for renewable energy microgrids. Sustainability“. 13(3), 1317, 2021.

[6.] J. Bao, D. He, M. Luo, and K. K. R. Choo, "A survey of blockchain applications in the energy sector". IEEE Systems Journal, 15(3), pp. 3370-3381, 2020.

[7.] Y. J. Lin, Y. C. Chen, J. Y. Zheng, D. Chu, D. W. Shao, and H. T. Yang, "Blockchain power trading and energy management platform". IEEE Access, 10, pp. 75932-75948.

[8.] N. Klaokliang, P. Teawtim, P. Aimtongkham, C. So-In and A. Niruntasukrat, "A novel IoT authorization architecture on hyperledger fabric with optimal consensus using genetic algorithm". In 2018 Seventh ICT International Student Project Conference, IEEE, ICT-ISPC, pp. 1-5, 2018.

[9.] G. Yang, K. Lee, K. Lee, Y. Yoo, H. Lee and C. Yoo, "Resource analysis of blockchain consensus algorithms in hyperledger fabric". IEEE Access, 10, pp. 74902-74920, 2022.

[10.] S. Liu, P. Viotti, C. Cachin, V. Quéma and M. Vukolić, "{XFT}: Practical fault tolerance beyond crashes". In 12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 16, pp. 485-500, 2016.

[11.] M. Castro, and B. Liskov, "Practical byzantine fault tolerance and proactive recovery". ACM Transactions on Computer Systems (TOCS), 20(4), pp. 398-461, 2002.

[12.] G. S. Veronese, M. Correia, A. N. Bessani, L. C. Lung and P. Verissimo, "Efficient byzantine fault-tolerance". IEEE Transactions on Computers, 62(1), 16-30, 2011.

[13.] Hyperledger Fabric, "Channels". (accessed: 2024.06.12) https://hyperledger-fabric.readthedocs.io/en/release-2.2/channels.html 2018.

[14.] J. Wang, and Z. Wang, "A survey on personal data cloud". The Scientific World Journal, 2014(1), 969150, 2014.

[15.] L. Lu, J. Han, Y. Liu, L. Hu, J. P. Huai, L. Ni, and J. Ma, "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps". IEEE Transactions on Parallel and Distributed Systems, 19(10), pp. 1325-1337, 2018.

[16.] A. Elli, C. Sharon, and F. Chris, "Private and confidential transactions with Hyperledger Fabric". (accessed: 2024.06.12) https://developer.ibm.com/tutorials/cl-blockchain-private-confidential-transactions-hyperledger-fabric-zero-knowledge-proof/ 2018.

[17.] B. Piedade, J. P. Dias, and F. F. Correia, "An empirical study on visual programming docker compose configurations". In Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings, pp. 1-10, 2020.