

Absztrakt

A kutatás során egy olyan rendszer került kifejlesztésre, amely a magyar Elektronikus Egészségügyi Szolgáltatási Tér hiányosságainak kezelésére szolgál. Az adatbiztonság érdekében az Ethereum blokklánc került alkalmazásra, amely védi a betegadatokat a manipulációtól. A munka során több hasonló rendszer került elemzésre, és a blokklánc-technológia részletes vizsgálata is elvégzésre került. Az elkészült rendszert alapos tesztelés követte, majd a kutatás összegzése és a további fejlesztési lehetőségek bemutatása történt meg.

Kulcsszavak

Blokklánc, Ethereum, Egészségügy, Solidity, MetaMask, Ganache

Motiváció

A kutatás célja egy decentralizált, blokklánc-alapú egészségügyi adatkezelő rendszer létrehozása, amely kiküszöböli az elektronikus egészségügyi rendszerek jelenlegi problémáit. A hagyományos, papíralapú betegadat-kezelés elavultsága és biztonsági kockázata, valamint a jelenlegi, központosított adatkezelési megoldások sebezhetősége (pl. EESZT) indokoltá tették egy megbízhatóbb alternatíva kidolgozását. Ez a portál a COVID világjárvány alatt Magyarországon kiemelt fontosságú volt, amely jelen kutatás fő motivációját adta. A blokklánc-technológia alkalmazásával egy olyan rendszer kerülhet kialakításra, amely nem függ központi szerverektől, így ellenállóbb a meghibásodásokkal és támadásokkal szemben. A kutatás alapját korábbi blokklánc-szimulációs vizsgálatok adták, amelyek segítettek a technológia elméleti és gyakorlati megértésében.

Hasonló fejlesztések

- **Blokklánc és IoT az orvosi adatok védelmére:** A Hyperledger Fabric alapú rendszer decentralizált módon tárolja a betegadatokat, biztosítva a biztonságos megosztást és védelmet. Az IoT-eszközök automatizáltan rögzítik a műtéti adatokat, megkönnyítve a későbbi kezeléseket.
- **MedRec: Ethereum-alapú egészségügyi adatrendszer:** A MedRec platform a blokkláncot csak az azonosításra és jogosultságkezelésre használja, míg az egészségügyi adatok helyi adatbázisokban maradnak. Okosszerződéseken keresztül szabályozza az adathozzáférést és értesítési rendszert biztosít.
- **Blokklánc szimuláció és vizualizáció:** Egy könnyűsúlyú blokklánc-szimuláció és tranzakciós gráf vizualizáció segíti a blokkláncok elemzését és modellezését. A kutatásban ezt az eszközt az adatelemzés és rendszerfejlesztés támogatására használták.

Sikerek

- 1 konferenciacikk

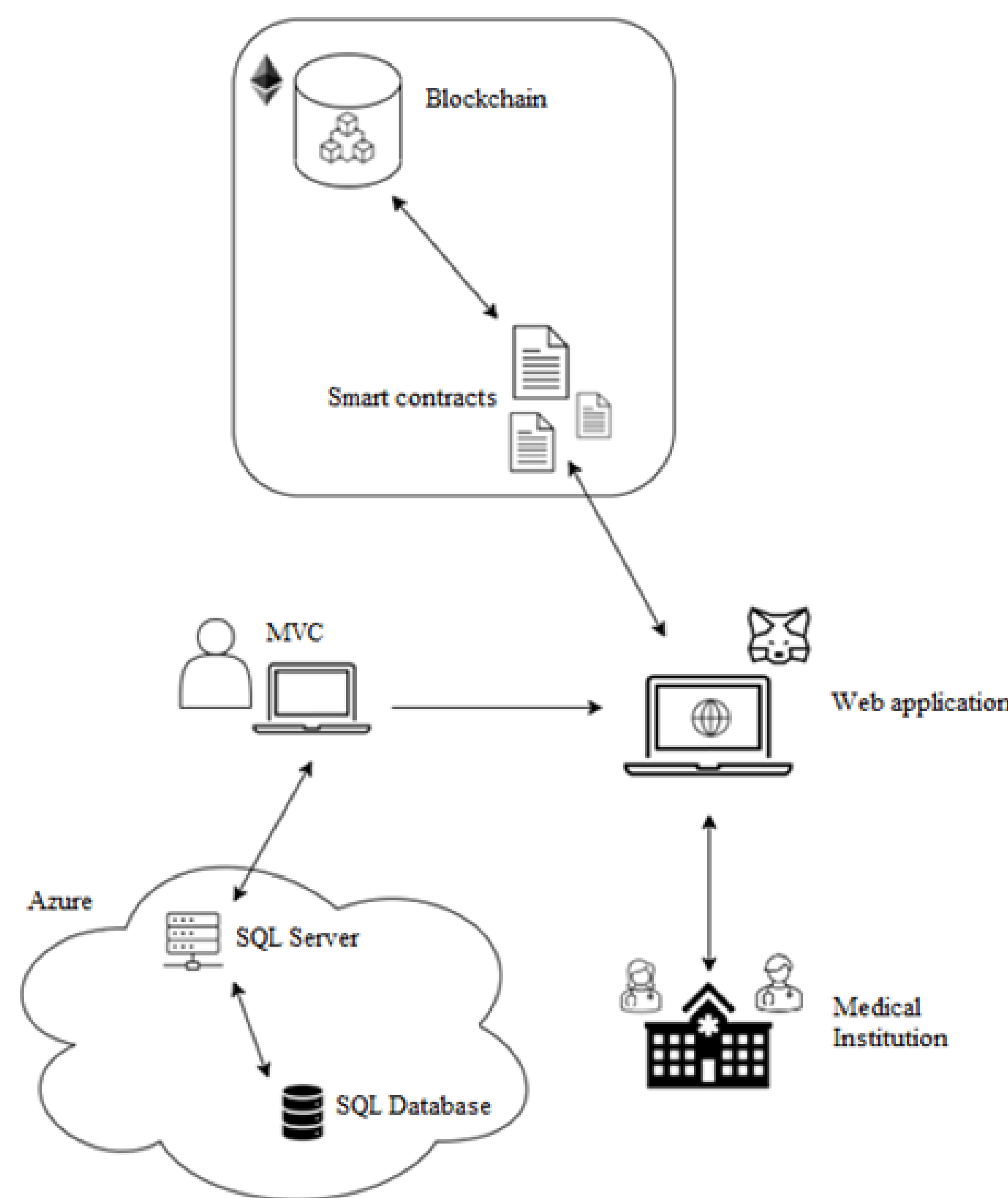
Saját módszer bemutatása

A fejlesztett rendszer egy biztonságos, blokklánc-alapú egészségügyi alkalmazás, amely Ethereum hálózaton fut, és Node.js környezetben készült. Az alkalmazás azonosítása kétlépcsős hitelesítést alkalmaz: a felhasználók először egy MVC alkalmazáson keresztül jelentkeznek be, majd a MetaMask segítségével tranzakciókat hajtanak végre.

A felhasználók jogosultságkezelése egy okosszerződésen keresztül történik, amelyben az orvosok és gyógyszerészek publikus címei és jelszavai tárolódnak, biztonságos, SHA-512 hash-alapú titkosítással. A hitelesítés után a DApp az adataikat a böngészőben tárolja, optimalizálva a teljesítményt.

A fejlesztési környezet Ganache privát blokkláncot használ, amely lehetővé teszi az okosszerződések telepítését és tesztelését. Négy különböző okosszerződés készült, amelyek a betegadatok és egészségügyi vizsgálatok kezeléséért felelnek. Az okosszerződések telepítési költsége egyértelmű összefüggést mutatott a komplexitásukkal: míg az egyszerűbb szerződések néhány ezer forintba kerültek, a legösszetettebb szerződés esetében ez az összeg több százezer forintra nőtt.

Eredmények értékelése



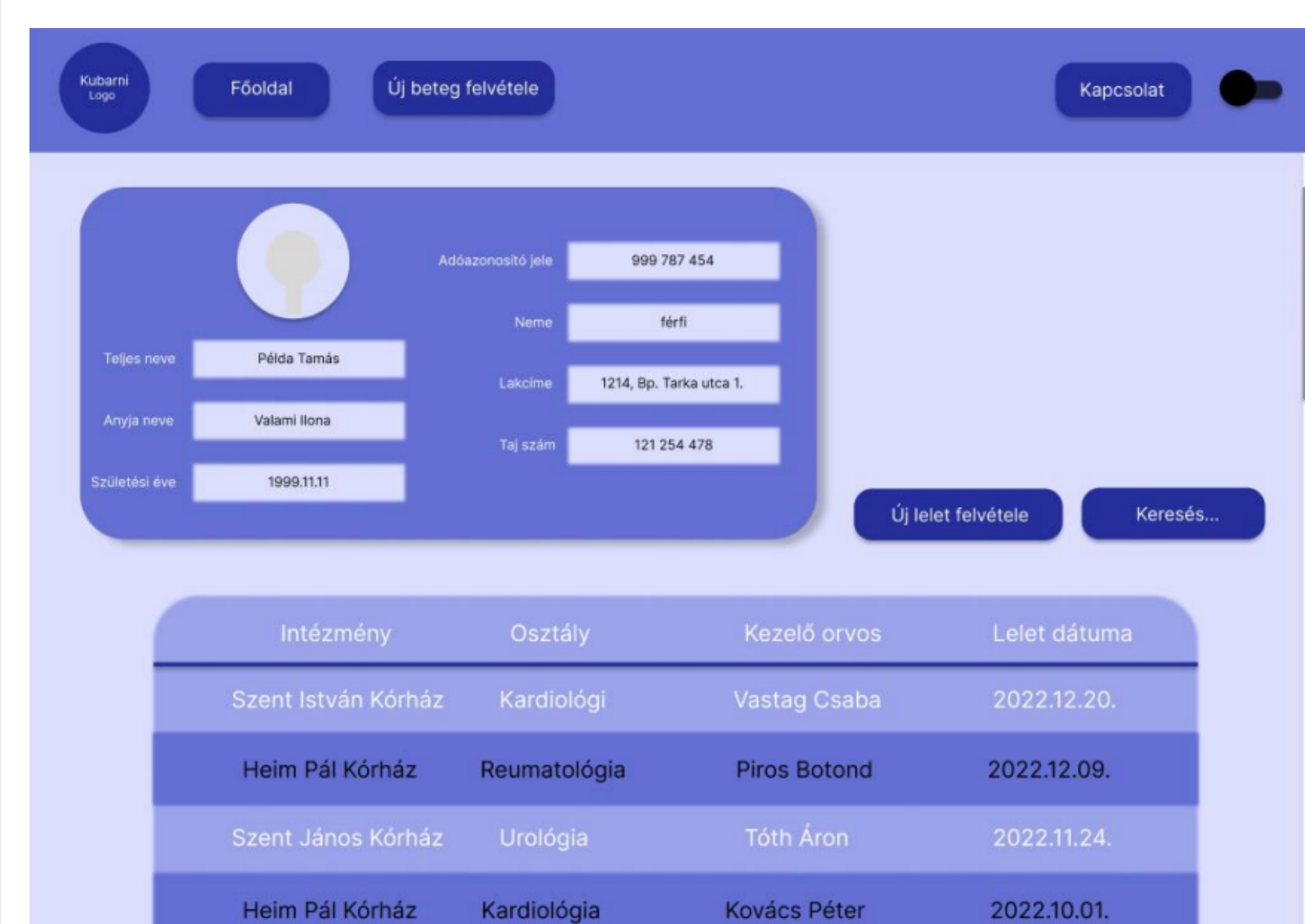
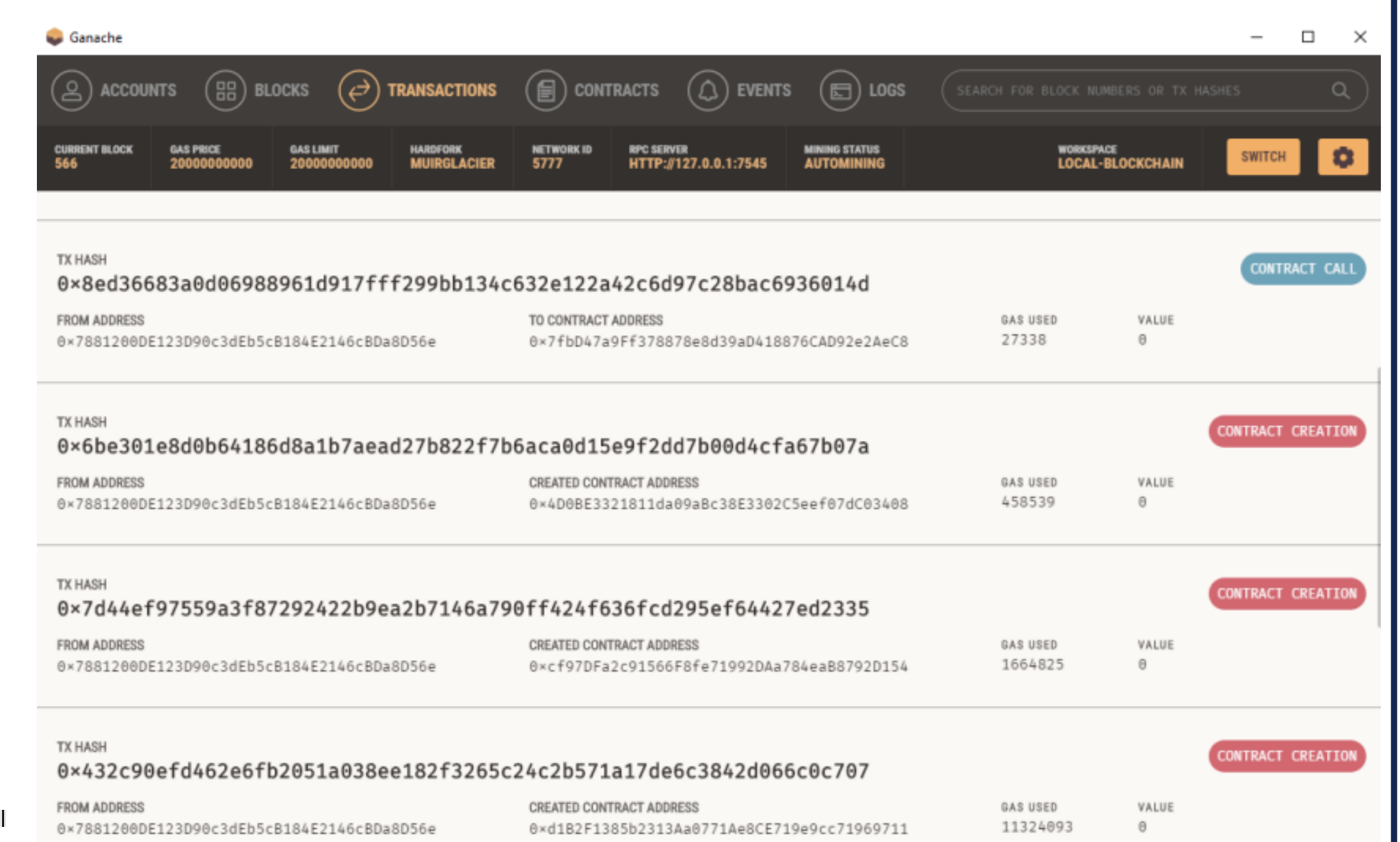
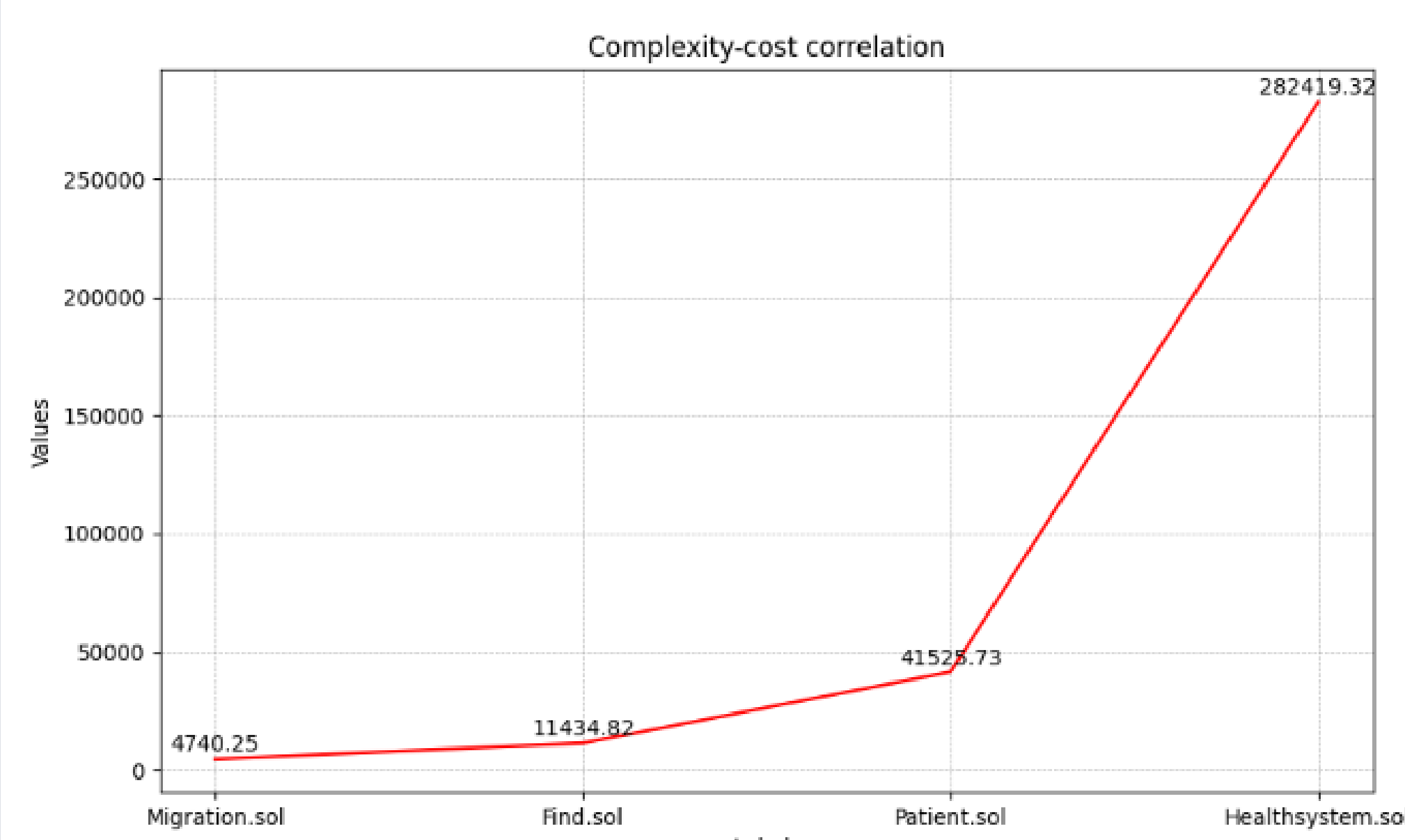
tését az 1. ábra mutatja be.

A teljesítményértékelés során két fő nehézség merült fel: a magas telepítési költségek miatt nem volt lehetőség a rendszer éles blokkláncon történő tesztelésére, és a decentralizált alkalmazások (DApp-ok) teljesítménye eltérő módon mérhető a hagyományos rendszerekhez képest.

Az Ethereum Virtuális Gép (EVM) teljesítménye két fő tényezőtől függ: az olvasási műveletek gyorsak és a felhőalapú adatbázisokhoz hasonlíthatók, míg az írási műveletek lassabbak és a bányászati folyamatokhoz kötöttek. Az írási sebesség fő befolyásoló tényezője a Gas díj, amely megfelelő egyensúly beállítását igényli a költségek és a tranzakciós sebesség között. A költségek és a kód komplexitás arányát a 2. ábra mutatja.

Bár a rendszer éles hálózaton nem került tesztelésre, más népszerű DApp-ok, például a KAI-CHING és az Alien Worlds példái azt mutatják, hogy az Ethereum blokklánc képes nagy terhelés kezelésére. Tekintettel Magyarország lakosságára és az egészségügyi tranzakciók becsült számára, valószínűsíthető, hogy a rendszer problémamentesen működhetne egy nyilvános hálózaton is.

A fejlesztett alkalmazás sikeresen megvalósította az eredeti célkitűzéseket, beleértve a betegek adatainak biztonságos tárolását és listázását a blokkláncban. A rendszer részeit és azok felépítését az 1. ábra mutatja be.



A kutatás során sikerült egy biztonságos, blokklánc-alapú egészségügyi rendszert létrehozni, amely megakadályozza az adatok manipulálását. A fejlesztés során blokklánc technológia kihívást jelentett, de sikerült egy működő megoldást kidolgozni. A tesztelés kiemelt szerepet kapott, a rendszer minden fő funkciója tesztelésre került. A kész rendszer egy nézetét a 4. ábra mutatja be, ahol egy beteghez tartozó vizsgálati betegadatok szerepelnek. Az itt eltárolt adatokat Ganache segítségével lehet megnézni, hogy a blokkláncban hogy tárolódik el (3. ábra).