

Abstract

O tehnologie inovativă folosită adesea în sectoarele financiar, medical, Internet of Things și multe altele, blockchain poate ajunge la un consens în cadrul unei rețele descentralizate - potențial compusă din multe noduri nesigure - și să stocheze în mod permanent și ireversibil datele. Această tehnologie are capacitatea de a crea multe oportunități de cercetare și inovații în afaceri. Luând în considerare aceste aspecte, în această teză propunem un ghid de implementare a aplicațiilor software bazate pe tehnologia blockchain. De asemenea, prezentăm o serie de implementări inovatoare aplicate în domeniile Sisteme de Transporturi Inteligente și medicină, soluții alternative la sistemele centralizate actuale.

Având în vedere că tehnologia blockchain este din ce în ce mai folosită într-o gamă variată de domenii, propunem o serie de recomandări care trebuie luate în considerare în cadrul procesului de proiectare a soluțiilor software ce au la bază blockchain. Punctele cheie prezentate stau la baza unei analize a cercetării efectuate până în prezent, fiind propusă și o clasificare a nivelelor arhitecturii. Ghidul este prezentat sistematic astfel încât dezvoltatorii să își dea seama dacă blockchain este cea mai bună soluție și, în caz afirmativ, cum să modeleze toate componentele necesare, cum ar fi actori, date, interacțiuni, funcționalități, performanță, eficiență, securitate și audibilitate, luând în considerare cadrul legislativ.

În ceea ce privește smart city, sistemul de navigație auto este una dintre principalele direcții de cercetare din domeniul Sisteme de Transporturi Inteligente, direcție care își propune să eficientizeze traficul și să calculeze rutele de călătorie. Aplicațiile existente, cum ar fi Google Traffic sau Waze, sunt adesea utilizate, dar pentru utilizatorii îngrijorați de datele lor personale, aceste sisteme sunt ca o cutie închisă. Folosind tehnologia blockchain, propunem arhitectura unui sistem de navigație auto în care protecția datelor personale este un pilon principal. Modelul a fost prezentat în cadrul "IEEE International Conference on Computational Science and Engineering" și a fost publicat în articolul "Blockchain privacy-preservation in Intelligent Transportation Systems". [1]

Al doilea model aplicat în cadrul Sistemelor de Transporturi Inteligente implementează un sistem de reputație bazat pe blockchain. Proiectul îi consideră actori principali ai arhitecturii pe utilizatorii interesați de informațiile despre trafic. Aceștia partajează în siguranță datele care sunt validate de către alți utilizatori. Utilizatorii pot alege să folosească astfel de date validate de mulțime sau date generate de sistem pentru a călători între două locații. Datele salvate sunt sigure, bazate pe reputația clienților și nu pot fi modificate. Prezentăm rezultatele simulării pentru trei orașe: San Francisco, Roma și Beijing. De asemenea, demonstrăm faptul că impactul atacurilor determină scăderea vitezei medii dacă informații eronate au fost stocate în blockchain, deoarece un algoritm de rutare îi ghidează pe utilizatorii onești pe alte rute libere și astfel aglomerează alte intersecții. Soluția este prezentată în articolul "Blockchain-based Reputation for Intelligent Transportation Systems". [2]

În domeniul medical, partajarea datelor, confidențialitatea și interoperabilitatea trebuie să fie preocupări majore. În prezent, niciun sistem informatic nu asigură toate aceste aspecte. Folosind tehnologia blockchain, descriem arhitectura unui sistem aplicat în medicină, sistem în care avem în vedere toate punctele cheie menționate. Propunerea noastră include toți actorii implicați, asigurând securitatea informațiilor salvate. Acest concept a fost prezentat în cadrul conferinței BDA 2018 "34th Conference on Data Management - Principles, Technologies and Applications" și publicat în "Proceedings of the BDA 2018 Conference" sub denumirea "Blockchain privacy-preserving in healthcare". [3]

În continuare prezentăm un design de sistem în care tehnologia blockchain este propusă a fi utilizată în sistemul medical, unde informațiile vitale referitoare la analizele medicale sunt

partajate între spitale, policlinici și institute de cercetare în funcție de politicile de acces definite de pacienți . Pentru a proteja datele confidențiale, soluția noastră implică utilizarea a două tipuri de blockchain: unul privat, sidechain, care păstrează informații despre ID-ul real al pacienților și unul public, mainchain, care stochează informații despre sănătatea pacienților, date marcate cu un ID temporar. Pentru a îl testa, am dezvoltat designul folosind platforma Hyperledger Fabric. Rezultatele experimentale prezintă o performanță bună a sistemului în raport cu următoarele valori: 1) timpul necesar pentru acceptarea unei noi tranzacții, 2) timpul de propagare a mainchain-ului tuturor nodurilor din rețeaua peer to peer și 3) timpul necesar pentru identificarea datelor medicale pentru un anumit pacient. Soluția a fost prezentată la conferința "IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)" și descrisă în articolul "Blockchain-based approach for e-health data access management with privacy protection". [4]