Fișă proiect instituțional pentru publicarea pe site-ul cercetare.ase.ro

(maxim 5 pagini)

Titlu proiect:

Votul electronic securizat prin tehnologia blockchain – aplicabilitate în alegerile din cadrul universităților

Instituția care a propus tema:

MODEX

Director:

DIACONIȚA Vlad, Profesor universitar

Echipa:

BELCIU Anda, Conferențiar universitar OPREA Simona Vasilica, Conferențiar universitar STOICA Maria Georgiana, Doctorand și Cadru didactic asociat BARBU Dragoș-Cătălin, Doctorand și Cadru didactic asociat BĂROIU Alexandru-Cătălin, Doctorand

Obiective:

Proiectul de cercetare și-a propus să răspundă la următoarele întrebări de cercetare: • Pentru vot electronic, care sunt avantajele și dezavantajele principalelor platforme blockchain, publice și private, care oferă suport pentru dezvoltarea de contracte de inteligente? • Poate fi folosită tehnologia blockchain pentru asigurarea faptului că doar persoanele care au drept de vot într-o anumită rundă de alegeri vor putea vota și vor putea vota o singură dată? Acest lucru implică că nici măcar administratorii de sistem sau administratorii bazei de date, nu poate schimba un buletin de vot sau genera noi voturi (de exemplu, pentru a mări voturile pentru un candidat). • Care sunt compromisurile dintre asigurarea secretului votului și asigurarea transparenței și implicit a unor modalități de audit al procesului electoral?

Activități:

Activitatea 1: Managementul proiectului și diseminarea rezultatelor prin realizarea unui raport de cercetare si transmiterea spre publicare a cel puțin 2 articole;
Activitatea 2: Analiza serviciilor de eGuvernare bazate pe blockchain și contextul european (sisteme de votare electronică, în particular);
Activitatea 3: Analiza arhitecturilor și modelelor de blockchain (model centralizat vs model distribuit, model PoW vs PoS, scalabilitate, securitate, stocare date on-chain și off-chain, sustenabilitate, consum) cu accent pe necesitățile unui sistem e-voting. Exemplu de bune practici - tehnologia KSI din Estonia – (primul sistem blockchain care deține acreditarea eIDAS – marca de încredere a UE pentru servicii calificate pentru tranzacțiile electronice pe Piața Unică
Activitatea 4: Analiza arhitecturilor implementate/propuse in cadrul universităților;
Activitatea 5: Propunerea unei arhitecturi (cerințe ale sistemului de votare, componentele cheie, model conceptual) și a unui token bazat pe un smart contract (SC) pentru un sistem e-voting;
Activitatea 6: Conceptualizarea și dezvoltarea de modele de ML care pot deservi un sistem de vot electronic securizat prin BC, cum ar fi modele de detectare a anomaliilor pentru a depista în timp real orice tentativă de fraudă electorală sau alte fenomene asemănătoare pornind de la date on-chain.

Rezultate:

În acest proiect, au fost analizate principalele platforme cu suport pentru Smart Contracts (SC) și au fost propuse mai multe soluții de vot bazate pe Blockchain (BC). Fiecare tip de platformă are cazurile sale de utilizare specifice, neexistând o platformă SC universală. Ethereum este de mult timp pe piață, are o comunitate mare de dezvoltatori și poate fi folosită gamă largă de scenarii de aplicații. În schimb, Internet Computer și Solana sunt platforme mai noi care pun accent pe performanță ridicată și scalabilitate iar soluții precum cele bazate pe blockchain tables sunt mai ușor de implementat în cadrul unor soluții cu baze de date existente. Votul electronic securizat prin BC poate fi o alternativă viabilă la votul în persoană și la votul prin corespondență mai ales pentru alegerile cu miză mică. Votul securizat prin BC ar putea fi prea riscant pentru alegeri politice cu mize mari în acest moment, deoarece SC și BC arată încă unele vulnerabilități și chiar un zvon ar putea zgudui considerabil încrederea publicului în sistem. Deși are limitările sale, iar îmbunătățirile viitoare sunt posibile, votul prin BC reprezintă o îmbunătățire față de votul electronic tradițional, în care utilizatorul se conectează la un site web și votează. Ca o dezvoltare viitoare, dovada identității fără cunoștințe anterioare (*zero-knowledge identity proof*) și criptarea homomorfă ar putea fi implementate, astfel încât un alegător să-și poată dovedi eligibilitatea la vot fără a dezvălui informații personale. Implementarea unor astfel de algoritmi ar putea îmbunătăți verificarea și confidențialitatea de la un capăt la altul și ar putea facilita accesul la alte servicii online ale universității. Ca o limitare, algoritmii *zero-knowledge identity proof* sunt încă lenți în comparație cu criptarea tradițională, așa că sunt greu de implementat la scară. Pentru a îmbunătăți și mai mult încrederea, sunt necesare cercetări viitoare privind verificarea formală a contractelor inteligente pentru a stabili standarde acceptabile de industrie pentru a verifica dacă codul SC nu conține erori și vulnerabilități.

In cadrul proiectului au fost publicate trei articole de cercetare:

[1] Diaconita Vlad, Anda Belciu, and Maria Georgiana Stoica. 2023. "Trustful Blockchain-Based Framework for Privacy Enabling Voting in a University" Journal of Theoretical and Applied Electronic Commerce Research 18, no. 1: 150-169, Jurnal Indexat WoS, Social Sciences Citation Index (SSCI), Category Business, Factor de Impact 5.318, AIS 0.462, https://doi.org/10.3390/jtaer18010008

[2] Dragoș-Cătălin BARBU, Gabriela DOBRIȚA (ENE), Simona-Vasilica OPREA, Adela BÂRA, Vlad DIACONIȚA, Challenges and benefits of Blockchain-based Electronic Voting System, Romanian Journal of Information Technology and Automatic Control, Vol. 32, No. 4, 117-128, 2022, Wos Emerging Sources Citation Index (ESCI), Computer Science, Interdisciplinary Applications, https://rria.ici.ro/wp-content/uploads/2022/12/art._Barbu_Dobri%C8%9Ba_Oprea_B%C3%A2ra...pdf

[3] Alexandru Costin BAROIU, Gabriela DOBRITA (Ene), Twitter Sentiment and Bitcoin Price - Is there a connection?, International Conference on System Theory, Control and Computing 2022, Conferință Indexată Wos, https://ieeexplore.ieee.org/document/9931814