Provocări și beneficii ale sistemului de vot electronic bazat pe Blockchain

Dragoș-Cătălin BARBU, Gabriela DOBRIȚA (ENE) , Simona-Vasilica OPREA, Adela BÂRA, Vlad DIACONIȚA

Departamentul de Informatică și Cibernetică Economică
Academia de Studii Economice din București

dragos.barbu@csie.ase.ro; gabriela.ene02@gmail.com; simona.oprea@csie.ase.ro; bara.adela@ie.ase.ro; diaconita.vlad@ie.ase.ro

Rezumat: Scopul principal al acestui studiu este de a evidenția numeroasele provocări cu care se confruntă sistemele de vot electronic. Tehnologia blockchain este o alternativă atractivă pentru sistemele convenționale de vot electronic, în special pentru funcționalități cum ar fi: sistem distribuit, non-repudiere și securitate. Blockchain a fost folosită în principal pentru a dezvolta aplicații de vot electronic, datorită beneficiilor de autentificare end-to-end. Analiza efectuată în cadrul articolului a permis definirea principalelor beneficii și provocări ale diferitelor sisteme. În ciuda beneficiilor votului online, aceste soluții introduc noi amenințări și o singură vulnerabilitate poate duce la manipulări la scară largă a voturilor.

Cuvinte cheie: blockchain, votare, securitate, sistem distribuit.

Challenges and benefits of Blockchain-based Electronic Voting System

Abstract: The main goal of this study is to highlight the many challenges that electronic voting systems faced. Blockchain technology is an attractive alternative to conventional electronic voting systems especially for functionalities such as distributed system, non-repudiation and security. Blockchain has been mainly used to develop electronic voting applications, due to the end-to-end authentication benefits. The analysis performed in this article allowed to define main benefits and challenges of various systems. Despite the online voting benefits, this solution introduce new threats and one single vulnerability can lead to large-scale manipulations of votes.

Keywords: blockchain, voting, security, distributed systems.

1. Aspecte introductive

Această lucrare este structurată după cum urmează: secțiunea 1 prezintă contextul și principalele concepte necesare pentru a înțelege discuția studiilor selectate; secțiunea 2 prezintă o discuție asupra lucrărilor recente în domeniul sistemelor de vot bazate pe blockchain; secțiunea 3 prezintă tehnologia KSI din Estonia ca un studiu de caz asupra rezultatelor cercetării și secțiunea 4 prezintă concluziile și observațiile finale.

Cercetări recente (Guardtime, 2018) sugerează că metoda tradițională de vot ridică o varietate de preocupări cu privire la egalitate, corectitudine și motivația alegătorilor. Astfel, pentru zonele în care au apărut probleme majore în sistemul democratic și unde tehnologiile au permis introducerea votului electronic, cercetătorii și guvernele au propus noi proceduri de vot care garantează un anumit grad de siguranță împotriva fraudei la vot.

Votul electronic poate crește fiabilitatea alegerilor și, spre deosebire de votul cu buletin clasic de vot, este îmbunătățită simultan eficiența votării și integritatea procesului. Votul electronic este utilizat în mod obișnuit în diferite contexte de decizie datorită flexibilității, ușurinței de acces și a costurilor reduse în comparație cu alegerile convenționale. Cu toate acestea, protocoalele sugerate pentru votul electronic prezintă riscul de supra-autoritate și manipulare, ceea ce poate determina duplicarea voturilor, votul fraudulos, probleme în securitatea datelor, de confidențialitate, de anonimat și transparența în domeniul de vot (Xiao et al., 2019).

https://doi.org/10.33436/v32i4y202210

Aparatul electronic de vot – EVM (Electronic Voting Machine) este o alternativă la problemele cu sistemul de vot clasic. Cu toate acestea, aparatul electronic de vot nu rezolvă problemele de securitate și de aceea nu este folosit la scară largă. Principala problemă a EVM constă în faptul că este relativ simplu să se injecteze un malware în dispozitiv (Yi, 2019). Un alt tip de vot este cel digital, care utilizează instrumente automate pentru a vota și care se împarte în: votul electronic și votul pe Internet. Votul electronic este reprezentant prin faptul că alegătorii folosesc o mașină de vot, iar votul pe Internet este locul în care folosesc un browser de Internet pentru a face acest lucru. Sistemele digitale de vot permit alegătorilor să voteze din orice loc din lume, dincolo de limitele de locație, oferindu-se astfel flexibilitatea, confidențialitatea, protecția și confortul la vot.

Blockchain este o tehnologie de securitate cibernetică asigurată matematic pentru identificarea rapidă și imuabilă a modificărilor datelor digitale și a dispozitivelor inteligente. Tehnologia Blockchain face posibilă descoperirea oricărei și a tuturor modificărilor aduse datelor digitale, oricât de mici, indiferent de către cine, imediat și fără eroare.

Există cercetări în desfășurare care aplică soluții bazate pe blockchain în diferite domenii cum ar fi: asistență medicală, logistică, finanțe și multe altele (Berdik et al., 2021). Votul electronic este unul dintre domeniile în care tehnologia blockchain (BC) poate avea un efect semnificativ. În realitate, vulnerabilitatea este atât de mare încât nu este fezabil să folosim doar votul electronic. Efectele pot fi de amploare dacă un sistem de vot electronic este compromis. Arhitectura unei rețele bazate pe BC asigură că frauda este foarte puțin fezabilă din punct de vedere conceptual, deoarece o rețea BC este deschisă, centralizată și condusă de consens. Prin urmare, este necesar să se ia în considerare proprietățile unice ale blockchain-ului.

Conceptul de utilizare a tehnologiilor BC pentru o rețea de vot online i se acordă un interes sporit (Khan et al., 2020), (Lee et al., 2016), (Pathak et al., 2021). Pentru cetățeni, în calitate de utilizatori finali, un model de vot electronic bazat pe BC nu ar diferi semnificativ de un sistem standard de vot electronic. Procesele care stau la baza celor două sisteme sunt totuși destul de diferite. Votarea printr-un sistem BC va folosi criptarea, putând fi în același timp complet deschisă și stocată în mod public nu pe un singur server, ci pe o întreagă rețea distribuită. Un vot criptat este validat prin mecanism de consens pe o rețea BC și fiecare vot este înregistrat de public pe copii distribuite ale registrului BC. Rețeaua de vot BC este descentralizată și complet deschisă, de aceea îi protejează pe alegători. Ceea ce înseamnă că toată lumea poate număra voturile în cazul votului electronic bazat pe BC dar nimeni nu știe cine cu cine a votat.

2. Sisteme de vot electronice bazate pe Blockchain

Votul este un domeniu de aplicare a tehnologiei BC în care cercetătorii caută să exploateze avantajele acesteia, cum ar fi: transparența, confidențialitatea și non-repudierea. Recent, inițiative precum utilizarea tehnologiei BC pentru alegeri sigure și verificabile au primit o atenție semnificativă prin utilizarea tehnologiei BC pentru sistemele de vot electronic (Khoury et al., 2018), (Sun et al., 2018), (Guardtime, 2018). Majoritatea propunerilor adoptă cadrul BC ca o bază de date centralizată imuabilă în care voturile pot fi stocate, oferind o serie de garanții de securitate (Wang et al., 2018).

Riscurile din cele trei sisteme de vot (clasic, vot electronic și vot electronic bazat pe BC) au fost evidențiate de către Jafar & Aziz (2021), împreună cu prezentarea avantajelor tehnologiei BC în sistemele de vot electronic, printre acestea numărându-se:

- *Transparență* - istoricul tranzacțiilor rămâne vizibil iar fiecare nod din rețea oferă o imagine de ansamblu completă a tranzacțiilor;
- *Evitarea fraudei, manipulării datelor și reducerea corupției* - modificările nedorite sunt ignorate deoarece înregistrarea este conținută în multe registre dispersate. Stocarea datelor în registre distribuite permite prevenirea corupției și manipulării incorecte a voturilor;
- *Creșterea încrederii, controlului și accesului la informații* - datorat păstrării permanente a înregistrărilor și prin verificarea datelor de către diferite noduri. Informațiile sunt stocate în mai multe locuri, ceea ce poate crește ușurința în accesare și viteza de acces a acestora.

În prezent există mai multe protocoale comerciale de vot electronic la distanță, și anume FollowMyVote (FollowMyVote, 2022), TIVI (Tivi, 2022) și Polys (Polys, 2022) - unele dintre ele au fost aplicate pentru votul informal sau consultativ, altele au fost desfășurate pentru votul la nivel regional sau național.

Dagher și colaboratorii au prezentat framework-ul BroncoVote pentru alegerile la scară universitară (Dagher et al., 2018). Sistemul este implementat pe blockchain-ul Ethereum și se bazează pe criptarea homomorfă Paillier pentru a asigura confidențialitatea alegătorilor. Pentru a cripta voturile și pentru a actualiza numărul de voturi, BroncoVote interacționează cu un server extern care efectuează operațiunile necesare.

Implementarea unui sistem național de vot electronic în Islanda este prezentat de către Hjalmarsson (Hjalmarsson et al., 2018). Se disting diferite roluri pentru actori și sunt analizate diferite cadre blockchain pentru implementare, printre care: Exonum, Quorum și Geth. Schema electorală prezentată cere fiecărui alegător să meargă într-un district care folosește un blockchain privat Ethereum.

În (McCorry et al., 2017) este prezentată de asemenea o implementare a rețelei de vot prin blockchain-ul Ethereum. Sunt implementate două contracte inteligente, unul pentru vot și unul pentru calculele criptografice. Este de remarcat faptul că limitările de la acel moment ale platformei Ethereum și costul contractelor implementate restrânge utilizarea acestei abordări la alegeri cu opțiuni limitate, inclusiv pentru un număr restrâns de alegători (mai puțin de cincizeci).

Din literatura de specialitate se observă că sistemele existente sunt divizate în funcție de arhitectura actuală a blockchain-ului. În cazul Islandei, echipa a sugerat o singură rețea blockchain mare, ale cărei noduri erau buletinele de vot de district efective din întreaga țară. Orice vot exprimat va trebui să ajungă la un consens în această rețea gigantică ceea ce poate conduce la întârzieri. Pentru a contracara acest lucru, se propune o arhitectură diferită care implică o aranjare ierarhică a diferitelor lanțuri, în care fiecare lanț reprezintă o secție de vot și, în unele cazuri, un întreg district (Khan et al., 2018). Dar prin acest lucru s-ar adăuga complexitate rețelei și ar trebui să se ajungă la un consens de mai multe ori atunci când o tranzacție este înregistrată. Prin urmare, se poate provoca congestie în rețea.

3. Tehnologia KSI Blockchain în Estonia

Tehnologia KSI – *Keyless Signature Infrastructure* – (Guardtime, 2017) este o metodă și o infrastructură de rețea distribuită la nivel global pentru emiterea și verificarea semnăturilor KSI. Spre deosebire de abordările tradiționale ale semnăturii digitale, de exemplu, infrastructura cu chei publice (PKI), care depind de criptografia cu chei asimetrice, KSI utilizează doar criptografia cu funcție hash (Guardtime, 2018) permițând verificării să se bazeze numai pe securitatea funcțiilor hash și pe disponibilitatea unui registru public, denumit în mod obișnuit blockchain.

O modalitate de a privi tehnologia BC este să o vedem ca pe un „praf de apărare digitală” (*digital defence dust)* ce acoperă toate datele și dispozitivele inteligente care trebuie protejate de accesul și utilizarea abuzivă. Astfel, fiecare modificare a datelor poate fi detectată instantaneu pe baza urmelor lăsate în modelul „prafului de apărare digitală” care acoperă datele.

Tehnologia BC folosită în Estonia oferă scalabilitate ridicată. Astfel, se pot acoperi și cantități mari de date cu „praf de apărare digitală”, din moment ce părțile blocurilor sunt conectate între ele folosind un cod verificabil matematic care conectează blocurile într-un lanț, și care nu poate fi schimbat fără a lăsa urme. Acesta poate fi găzduit pe un număr mare de computere din întreaga lume și, prin urmare, poate fi controlat și verificat de un număr mare de părți.

Blockchain-ul KSI realizează o înregistrare publică distribuită a evenimentelor, adică o înregistrare ce permite numai adăugarea evenimentelor în care fiecare eveniment nou este legat criptografic de precedentul. Noile intrări sunt create folosind un protocol de consens distribuit.

Blockchain-ul KSI depășește două slăbiciuni majore ale blockchain-urilor tradiționale, făcându-l utilizabil la scară industrială:

- *Scalabilitatea*: una dintre cele mai semnificative provocări ale abordărilor tradiționale de tip blockchain este scalabilitatea – acestea cresc liniar odată cu numărul de tranzacții. În contrast, blockchain-ul KSI crește liniar în timp și independent de numărul de tranzacții;

- *Timpul pentru consens*: spre deosebire de abordarea pe scară largă a criptomonedelor, numărul de participanți la protocolul de consens distribuit blockchain KSI este limitat. Prin limitarea numărului de participanți, devine posibilă obținerea consensului în mod sincron – eliminând necesitatea PoW (*Proof of Work)* și asigurându-se că acest consens poate avea loc în decurs de o secundă.

Diferențele dintre KSI, Bitcoin și RSA sunt evidențiate în tabelul de mai jos:

Tabel 1. Diferențe KSI – Bitcoin - RSA

	KSI	Bitcoin	RSA
Scalabilitate	globală, liniară în timp	globală, liniară în funcție de numărul de tranzacții	locală
Timp pentru consens	sub 1 secundă	nedeterminist, 5-15 min	sub 1 secundă
Confidențialitatea datelor	Datele nu sunt divulgate niciodată	Datele sunt adăugate la blockchain	Datele nu sunt divulgate niciodată
Managementul cheilor	N/A	N/A	Este necesar

Unii furnizori de blockchain - cum ar fi Guardtime, o companie din spatele blockchain-ului KSI folosit de Estonia - au mers chiar dincolo de asta și publică blockchain-ul și în mass-media, cum ar fi ziarul Financial Time (Buldas et al., 2020). Dacă cineva ar dori să manipuleze blockchain-ul KSI fără ca nimeni să observe, nu numai că ar trebui să se ocupe de „praful de apărare digitală" din domeniul electronic, ci și să înlocuiască zeci de mii de copii ale ziarelor din bibliotecile lumii. Este clar că nimeni – nici măcar Guardtime în sine – nu este capabil să facă asta și, prin urmare, datele de pe blockchain pot fi considerate imuabile.

Când aveți de-a face cu orice fel de date sensibile, este evident că acestea nu trebuie păstrate pe blockchain deoarece blockchain se bazează pe un număr mare de ochi pentru a le menține în siguranță. În schimb, pentru a securiza datele sensibile, ceea ce este păstrat pe blockchain pot fi doar „valorile hash" - în esență amprentele digitale ale datelor originale. Așa cum propriile amprente ne reprezintă în mod unic, același lucru se aplică și în cazul amprentelor digitale - deși reprezintă în mod unic datele originale, este imposibil să afli ceva despre datele în sine pe baza „valorilor hash".

Estonia este un adevărat pionier în soluțiile de guvernare electronică, fiind numită „cea mai avansată societate digitală din lume" de către Wired (Hammersley, 2017). Statul baltic a construit un ecosistem eficient, sigur și transparent, economisind atât timp cât și bani pentru populație, precum și pentru sistemul public. Cu aproximativ două decenii în urmă, când societatea informațională începea să se dezvolte în Estonia, datele digitale despre cetățenii estonieni nu erau colectate. Populația nu avea acces la Internet sau chiar dispozitive care să permită accesul la acesta. A fost nevoie de mult curaj și viziune din partea statului estonian pentru a investi în soluții de tehnologia informației (IT) și a face primii pași inovatori pe drumul tehnologiei informației, pași care au transformat acum Estonia într-una dintre cele mai dezvoltate societăți digitale din lume.

Cu toate acestea, a fi o societate digitală înseamnă a te expune amenințărilor cibernetice. Urmare a experienței Estoniei din 2007 cu privire la atacurile cibernetice (Ottis, 2008), a fost adoptată tehnologia BC pentru asigurarea integrității datelor stocate în depozitele guvernamentale și pentru a proteja aceste date împotriva amenințărilor interne și externe. Prin arhitectura KSI Blockchain, implementată în rețelele guvernamentale estoniene, istoricul datelor nu poate fi rescris de nimeni, iar autenticitatea datelor electronice poate fi dovedită matematic. Ceea ce înseamnă că nimeni – nici hackerii, nici administratorii de sistem și nici măcar guvernul în sine – nu poate manipula datele fără a lăsa urme.

Odată cu a patra revoluție industrială, importanța promovării soluțiilor blockchain devine din ce în ce mai evidentă. Investițiile solide în infrastructura de securitate cibernetică au ajutat Estonia să dezvolte o expertiză extinsă în acest domeniu, devenind una dintre cele mai recunoscute și valoroase surse de expertiză internațională în domeniul securității cibernetice.

După ce a făcut primii pași pentru a deveni un stat electronic, Estonia și-a dat seama că riscul atacurilor cibernetice va face întotdeauna parte din societatea informațională – un risc care trebuie luat în serios. După analizarea diferitelor opțiuni, Estonia a găsit o soluție pentru aceasta – tehnologia BC - o soluție de securitate cibernetică asigurată matematic pentru identificarea utilizării și a folosirii greșite a datelor digitale și a dispozitivelor inteligente, oferind transparență și fiabilitate tuturor organizațiilor și instituțiilor din sectorul public sau privat care lucrează cu date digitale sau dispozitive inteligente.

Deși BC a devenit un subiect de actualitate abia în ultimii ani, Estonia a început să testeze tehnologia din 2008 – chiar înainte de publicarea Cărții albe Bitcoin (Nakamoto, 2008), care a inventat prima dată termenul „blockchain”. La acea vreme, în Estonia, această tehnologie era denumită „marcare temporală legată de hash”. Iar din 2012, tehnologia BC a fost utilizată în producție pentru a proteja datele naționale, serviciile electronice și dispozitivele inteligente atât în sectorul public cât și în cel privat.

Deși originea academică a Bitcoin este adesea necunoscută, criptografia din spatele acelor componente individuale este bine cunoscută încă din anii 1990 (Bayer et al., 1993), iar criptografii Guardtime au fost participanți foarte activi în acest domeniu.

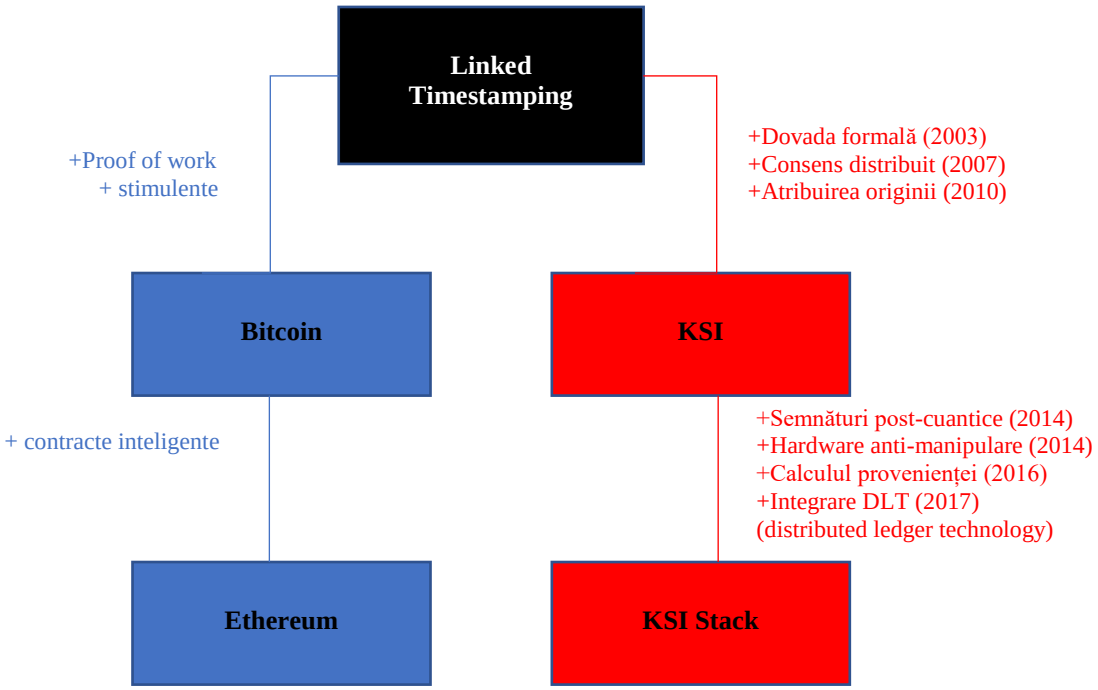

Figura 1. Arborele genealogic al tehnologiei blockchain.
Sursă https://guardtime.com/technology

Unul dintre conceptele de bază din spatele bitcoin se numește „marcare temporală înlănțuită (*linked timestamping*)”(evoluția genealogică fiind evidențiată în figura 1), iar profesorii Ahto Buldas și Märt Saarepera de la Guardtime au fost primii criptografi care au oferit o dovadă formală de securitate în 2003, adică au definit ce proprietăți sunt necesare pentru funcțiile hash și structurile de date pentru a construi o dovadă de securitate verificabilă formal (Buldas et al., 2004).

Compania estonă de blockchain Guardtime a fost lansată în 2007 cu scopul de a crea un sistem de securitate verificabil formal pentru guvernul eston, adică eliminarea terților, a persoanelor de încredere din interior sau a cheilor criptografice în verificarea integrității înregistrărilor, rețelelor și sistemelor guvernamentale.

Provocarea nu era de ordin criptografic, ci de inginerie, astfel se dorea construirea unui serviciu scalabil și de încredere pentru guvern care va continua să funcționeze chiar și în cazul unui atac cibernetic constant.

Drept urmare, sistemul a avut succes și a intrat în producție în aprilie 2008, iar în ultimul deceniu, Guardtime a continuat să inoveze, adăugând din ce în ce mai multe funcționalități platformei (Fig. 2) . Guardtime a adăugat semnături post-cuantice pentru a înlocui RSA, hardware-ul Anti-Tamper (*Black Lantern*), un calcul al provenienței conceput pentru a urmări și monitoriza infor-mațiile digitale pe măsură ce depășesc granițele organizaționale, și multe alte caracteristici noi (Guardtime, 2018).

Rezultatul este o mulțime de tehnologii, concepute în spiritul filozofiei Unix – abstractizare și încapsularea funcționalității în straturi. Guardtime oferă o stivă de blockchain de la un capăt la celălalt, astfel, de la infrastructura fizică la middleware, și în final la pachete de soluții.

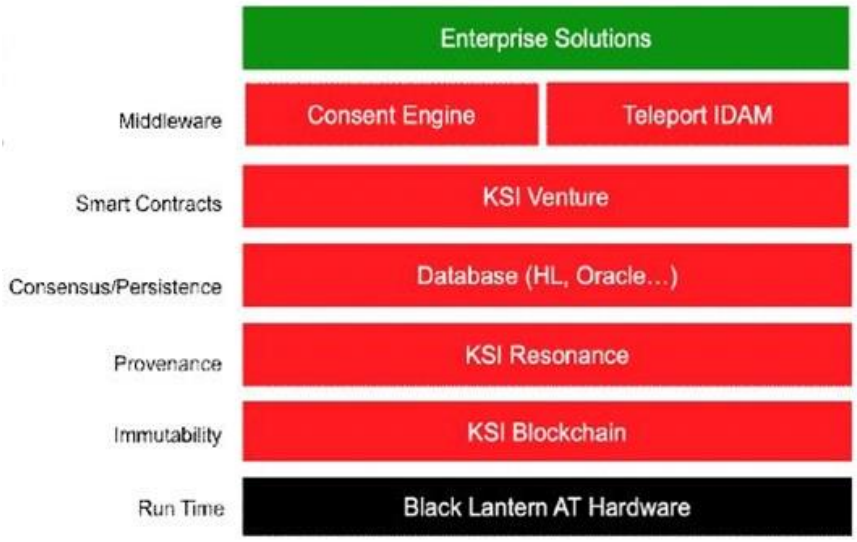

Figura 2. Stiva KSI

Tehnologia KSI Blockchain, dezvoltată de Guardtime, este proiectată în Estonia și utilizată la nivel global pentru a se asigura că rețelele, sistemele și datele nu sunt compromise, toate păstrând confidențialitatea 100% a datelor.

Beneficiile KSI includ (KSI, 2017):

- *Dimensiune mare*. Semnăturile KSI pot fi generate pe date la nivel de exabyte. Chiar dacă un exabyte de date (1.000 de petaocteți) este generat în jurul planetei în fiecare secundă, fiecare înregistrare de date (un trilion de înregistrări presupunând o dimensiune medie de 1 MB) poate fi semnată utilizând KSI cu cheltuieli de calcul, stocare și rețea neglijabile.
- *Portabilitate*. Proprietățile datelor semnate pot fi verificate chiar și după ce datele respective au depășit granițele geografice sau organizaționale și chiar a furnizorilor de servicii.
- *Confidențialitatea datelor*. KSI nu trece prin procesul de ingestie a datelor clienților; datele nu părăsesc niciodată sediul clientului. În schimb, sistemul se bazează pe funcții hash criptografice unidirecționale care au ca rezultat valori hash reprezentând în mod unic datele. Acestea sunt ireversibile, astfel încât nu se poate începe cu valoarea hash pentru reconstruirea datele - astfel, confidențialitatea datelor este garantată în orice moment.
- *Verificare independentă*. Proprietățile datelor semnate pot fi verificate fără a avea nevoie de o autoritate de încredere.

În Estonia, tehnologia blockchain ajută la detectarea celor care se uită la datele digitale de sănătate ale unei persoane, cine le modifică și când. Pentru a păstra informațiile de sănătate

complet securizate și, în același timp, accesibile persoanelor autorizate, se utilizează sistemul electronic de carte de identitate. În acest fel, fiecare apariție a utilizării eronate a datelor este detectabilă și pot fi prevenite daune majore pentru sănătatea unei persoane (cum ar fi medicamentul greșit sau doza greșită).

Aceeași tehnologie KSI Blockchain este utilizată de Centrul de Excelență pentru apărare cibernetică cooperativă NATO, Agenția IT a Uniunii Europene, Departamentul de Apărare al SUA și, de asemenea, de companiile Verizon, Lockheed Martin, Maersk, Ericsson, Ernst&Young și alții.

Conform cercetării efectuate de FireEye, unul dintre cei mai importanți furnizori de securitate cibernetică din lume, în prezent organizațiile necesită în medie aproximativ 7 luni pentru a detecta încălcările și manipulările datelor electronice. Cu soluția blockchain precum cea pe care o folosește Estonia, aceste încălcări și manipulări pot fi detectate imediat.

Pentru a implementa blockchain-ul în sistemele informaționale ale statului Estoniei, Autoritatea Estoniană pentru Sisteme Informaționale (RIA), în calitate de furnizor intern de servicii pentru guvern, garantează accesul la rețeaua BC pentru agențiile de stat prin infrastructura X-Road (https://e-estonia.com/) fiind o arhitectură descentralizată. X-Road este un mediu tehnologic și organizațional care permite schimbul securizat de date pe Internet între sistemele de informații și se bazează pe un ecosistem interoperabil. X-Road este implementat și în Finlanda, Azerbaidjan, Namibia și Insulele Feroe și permite schimbul automat de date între țări. Din 2017 a fost stabilită capacitatea de schimb automat de date între Estonia și Finlanda.

4. Concluzii

Acest articol oferă o privire de ansamblu asupra sistemelor de vot electronic bazate pe tehnologia blockchain. Prin analiza noastră, examinăm starea actuală a sistemelor de vot bazate pe blockchain și orice dificultăți asociate cu care se confruntă pentru dezvoltarea viitoare. Cele mai des menționate probleme în aplicațiile blockchain sunt protecția confidențialității și viteza tranzacțiilor. Securitatea participării la distanță trebuie să fie viabilă și, pentru scalabilitate, viteza tranzacțiilor trebuie să i se acorde o atenție sporită.

Ritmul de schimbare al tehnologiei este foarte rapid, acest lucru fiind valabil și în industria blockchain. Este important să înțelegem natura, beneficiile și cazurile de utilizare ale tehnologiei blockchain, cât și să luăm în considerare concepțiile sale greșite și provocările viitoare, acest lucru având un impact asupra implementării și dezvoltării mai ample în industrie. Prezentarea tehnologiei KSI din Estonia a fost detaliată fiind un studiu de caz prin care se dovedește viabilitatea unui sistem de vot electronic bazat pe blockchain și aplicarea tehnologiei blockchain în sistemele informaționale.

Acest studiu a arătat că sistemele blockchain au ridicat probleme care necesită mai multă atenție și există încă multe probleme tehnice care trebuie abordate înainte de implementarea unui sistem de vot electronic bazat pe blockchain.

Mulțumiri

Cercetarea a fost finanțată de către Academia de Studii Economice din București, proiect instituțional nr. 323/2022, “Votul electronic securizat prin tehnologia blockchain – aplicabilitate în alegerile din cadrul universităților”.

BIBLIOGRAFIE

1. Bayer, D., Haber, S. & Stornetta, W. S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping In: Capocelli, R., De Santis, A. & Vaccaro, U. (eds), *Sequences II*, 329–334. Springer, New York, NY, doi: 10.1007/978-1-4613-9323-8_24.
2. Berdik, D. O. S. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1): 102397, doi: 10.1016/j.ipm.2020.102397.
3. Buldas, A. & Saarepera, M. (2004). *On Provably Secure Time-Stamping Schemes. Advances in Cryptology - ASIACRYPT 2004*, 500–514. Springer Berlin Heidelberg, doi: 10.1007/978-3-540-30539-2_35.
4. Buldas, A., Draheim, D., Nagumo, T. & Vedeshin, A. (2020). *Blockchain Technology: Intrinsic Technological and Socio-Economic Barriers*, 3-27.
5. Dagher, G. G., Marella, P. M., Milojkovic, M. & Mohler, J. (2018). BroncoVote: Secure Voting System using Ethereum's Blockchain. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, doi: 10.5220/0006609700960107.
6. FollowMyVote (2022). *Secure Decentralized Application Development.* https://followmyvote.com/ [Accesat 15 decembrie 2022].
7. Guardtime (2017). *Keyless Signature Infrastructure Technology*. Guardtime Federal, LLC Proprietary.
8. Guardtime (2018). *Technology of Guardtime*. Guardtime Federal, LLC Proprietary. Online. https://guardtime.com/technology.
9. Hammersley, H. (2017). Concerned about Brexit? Why not become an e-resident of Estonia. *WIRED*. Online. https://www.wired.co.uk/article/estonia-e-resident.
10. Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M. & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, (pp. 983-986), doi: 10.1109/cloud.2018.00151.
11. Jafar, U. & Aziz, M. J. A. (2021). A State of the Art Survey and Research Directions on Blockchain Based Electronic Voting System. *Communications in Computer and Information Science*, 248–266. Springer Singapore, doi: 10.1007/978-981-33-6835-4_17.
12. Khan, K. M., Arshad, J. & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research*, 14(1), 53-62, doi: 10.4018/IJEGR.2018010103.
13. Khan, K. M., Arshad, J. & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, 105, 13–26, doi: 10.1016/j.future.2019.11.005.
14. Khoury, D., Kfoury, E. F., Kassem, A. & Harb, H. (2018). Decentralized Voting Platform Based on Ethereum Blockchain. *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*, (pp. 1-6), doi: 10.1109/imcet.2018.8603050.
15. Lee, K., James, J., Ejeta T. & Kim, H. (2016). Electronic Voting Service Using Block-Chain, *Journal of Digital Forensics, Security and Law, 11*, Article 8, doi: 10.15394/jdfsl.2016.1383.
16. McCorry, P., Shahandashti, S. F., Hao, F., Haber, S. & Stornetta, W. S. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *Journal of Cryptology*, 357–375.
17. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org.

18. Ottis, R. (2008). Analysis of the 2007 cyber attacks against estonia from the information warfare perspective. In *7th European Conference on Information Warfare and Security - ECIW 2008*, (pp. 163-168).

19. Pathak, P. M., Suradkar, A., Kadam, A., Ghodeswar, A. & Parde P. (2021). Blockchain Based E-Voting System, *International Journal of Scientific Research in Science and Technology*, 134-140, doi: 10.32628/ijsrst2182120.

20. Polys (2022). *Blockchain-based online voting*. https://polys.vote/ [Accesat 15 decembrie 2022].

21. Shahzad, B. & Crowcroft, J. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access, 7*, 24477–24488, doi: 10.1109/access.2019.2895670.

22. Sun, X., Wang, Q., Kulicki, P. & Sopek, M. (2018). A Simple Voting Protocol on Quantum Blockchain. *International Journal of Theoretical Physics*, 58(1), 275–281, doi: 10.1007/s10773-018-3929-6.

23. Tivi (2022). *TIVI powered by Smartmatic and Cybernetica*. https://tivi.io/ [Accesat 15 decembrie 2022].

24. Wang, B., Sun, J., He, Y., Pang, D. & Lu, N. (2018). Large-scale Election Based On Blockchain. *Procedia Computer Science, 129*, 234-237, doi: 10.1016/j.procs.2018.03.063.

25. Xiao, S., Wang, X. A., Wang, W. & Wang, H. (2019). *Survey on Blockchain-Based Electronic Voting*. *Advances in Intelligent Networking and Collaborative Systems*, 559-567. Springer International Publishing, doi: 10.1007/978-3-030-29035-1_54.

26. Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, 2019(1), doi: 10.1186/s13638-019-1473-6.

Dragoș-Cătălin BARBU este doctorand în cadrul Academiei de Studii Economice din București, în domeniul „Informatică Economică”, a absolvit Facultatea de Matematică și Informatică din cadrul Universității din București și deține o diplomă de master în domeniul ,,Informaticii Teoretice” din cadrul Departamentului de Informatică, Facultatea de Matematică și Informatică, Universitatea din București. În prezent deține funcția de Șef Serviciu „Cloud Computing” și este Cercetător Științific gradul III în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București, desfășurând activitate de cercetare în domeniul TIC de peste 15 ani. Este reprezentant supleant al României în Consiliul de conducere al Întreprinderii Comune Europene de calcul de înaltă performanță (EuroHPC JU) și, de asemenea, delegatul supleant al organizației mandatate de România în cadrul Asociației European Open Science Cloud (EOSC-A). A coordonat proiecte naționale în domeniul „Cloud Computing”, securitate informatică, servicii electronice, librării digitale, inteligență artificială și realitate îmbogățită, a participat la realizarea a peste 25 de proiecte naționale, 10 proiecte internaționale, și a publicat peste 35 de articole la nivel național și internațional.

Dragoș-Cătălin BARBU is a Ph.D. candidate at the University of Economic Studies in Bucharest, he graduated from the Faculty of Mathematics and Computer Science at the University of Bucharest and holds a master's degree in the field of Theoretical Informatics from the Department of Computer Science, the Faculty of Mathematics and Computer Science, the University of Bucharest. He is the Head of the "Cloud Computing" Department and a Senior Researcher III within the National Institute for Research and Development in Informatics – ICI Bucharest. Dragoș-Cătălin Barbu has been carrying out research activity in the ICT field for over 15 years, coordinating national projects in the field of "Cloud Computing", computer security, electronic services, digital libraries, artificial intelligence and augmented reality. He is the Romanian Substitute Representative in the Governing Board of European High Performance Computing Joint Undertaking (EuroHPC JU) and also the substitute delegate of Mandated Organisation by Romania in the European Open Science Cloud (EOSC-A) Association. Moreover, he participated in the implementation of more than 25 national projects, 10 international projects and he has published over 35 articles at a national and international level.

Gabriela DOBRIȚA (ENE) a absolvit Facultatea de Cibernetică, Statistică și Informatică Economică din cadrul Academiei de Studii Economice din București, în anul 2012, iar studiile de masterat în domeniul Informatică Economică în anul 2017. În prezent este doctorand în cadrul aceleiași universități. Principalele domenii de interes sunt: tehnologiile big data, data mining, inteligență artificială, algoritmi și structuri de date.

Gabriela DOBRIȚA (ENE) graduated from the Faculty of Cybernetics, Statistics and Economic Informatics in 2012, and received her master's degree in the field of Economic Informatics in 2017. She is currently a Ph.D. student in the field of Machine Learning at the same university. The main areas of interest are big data technologies, artificial intelligence, algorithms, and data structures.

Simona-Vasilica OPREA este conf. dr. univ. și profesor la Facultatea de Cibernetică, Statistică și Informatică Economică din cadrul Academiei de Studii Economice din București. Predă Baze de date, Sisteme de gestiune a bazelor de date și Pachete software. Deține diploma de master prin Programul de Management al Infrastructurii de la Universitatea Națională Yokohama, Japonia, în 2007. Primul doctorat este în Ingineria Sistemelor Energetice de la Universitatea

Politehnică din București în 2009, iar al doilea doctorat în Informatică Economică de la Academia de Studii Economice din București în 2017.

Simona-Vasilica OPREA is a Ph.D. Associate Professor, teaches Databases, Database Management Systems, and Software Packages at the Faculty of Economic Cybernetics, Statistics, and Informatics of the Bucharest University of Economic Studies. She received the MSc degree through the Infrastructure Management Program from Yokohama National University, Japan, in 2007, the first Ph.D. degree in Power System Engineering from the Bucharest Polytechnic University in 2009, and the second Ph.D. degree in Economic Informatics from the Bucharest University of Economic Studies in 2017.

Adela BÂRA a absolvit Facultatea de Cibernetică, Statistică și Informatică Economică, din cadrul Academiei de Studii Economice din București, în anul 2002, și a obținut doctoratul în cibernetică în anul 2007. În prezent este profesor la Catedra de Informatică Economică, Facultatea de Cibernetică, Statistică și Informatică Economică, din cadrul aceleiași universități. A coordonat patru Proiecte de Cercetare-Dezvoltare și a publicat peste 100 de lucrări în reviste și conferințe internaționale. Interesele ei de cercetare includ data science, analiza volumelor mari de date (big data) și machine learning.

Adela BÂRA received the degree from the Faculty of Economic Cybernetics, in 2002, and the Ph.D. diploma degree in economics, in 2007. She is currently a Professor with the Economic Informatics Department, Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest University of Economic Studies and coordinated three Research and Development Projects. She has authored more than 70 papers in international journals and conferences. Her research interests include data science, analytics, databases, big data, data mining, and power systems.

Vlad DIACONIȚA a absolvit în 2005 Facultatea de Informatică Economică în cadrul Academiei de Studii Economice din București, România. Din anul 2010 deține o diplomă de doctor în domeniul Cibernetică și Statistică în economie. Interesele sale sunt în principal în domeniul bazelor de date, depozitelor de date, big data, integrarea sistemelor, suport pentru decizii, învățarea

automată, cloud computing și energiile regenerabile. Este membru al IEEE (Computer Society), ACM și INFOREC și în prezent este editor asociat pentru IEEE Access.

Vlad DIACONIȚA graduated in 2005 the Economic Informatics program from The Bucharest University of Economic Studies, Romania. Since 2010 holds a Ph.D. in the domain of Cybernetics and Statistics in Economics. His interests are mainly in the domain of databases, data warehouses, big data, system integration, decision support, machine learning, cloud computing and renewable energies. He is a member of IEEE (Computer Society), ACM and INFOREC and currently serving as an Associate Editor for IEEE Access.